TaskSmart N2400

Administration Guide

Second Edition (January 2001)
Part Number 177675-002
Compaq Computer Corporation

Notice

© 2001 Compaq Computer Corporation

Compaq, the Compaq logo, Compaq Insight Manager, SANworks, SmartStart, ActiveAnswers, SoftPaq and ROMPaq Registered in U.S. Patent and Trademark Office. TaskSmart, CarePaq, and Tru64 are trademarks of Compaq Information Technologies Group, L.P. in the United States and other countries.

Microsoft, MS-DOS, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States and other countries.

Intel, Pentium, and Itanium are trademarks of Intel Corporation in the United States and other countries.

The Open Group and UNIX are trademarks of The Open Group in the United States and other countries.

All other product names mentioned herein may be trademarks of their respective companies. Compaq shall not be liable for technical or editorial errors or omissions contained herein. The information in this document is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for Compaq products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

Compaq TaskSmart N2400 Administration Guide
Second Edition (January 2001)
Part Number 177675-002

Contents

About This Guide

Text Conventions ix
Symbols in Text x
Symbols on Equipment x
⚠ Important Safety Information xi
Rack Stability xii
Getting Help xii
    Compaq Technical Support xii
    Compaq Website xiii
    Compaq Authorized Reseller xiii

Chapter 1

Initialization

Overview 1-1
Preinitialization: Before You Begin 1-2
    Verify That Hardware Installation Is Complete 1-2
    Initialization Methods 1-2
    Collect Information for Initialization 1-3
Task 1: Create the Configuration Data Diskette 1-4
Task 2: Remove the Front Bezel 1-6
Task 3: Insert the Configuration Data Diskette into the Server 1-7
Task 4: Connect the Standard Ethernet Cables 1-8
Task 5: Power Up the Server 1-10
Task 6: Monitor the Initialization Process 1-11
Task 7: Complete the System Configuration 1-13
    Required Configuration for All Work Environments 1-13
    Required Configuration by Work Environment 1-14
    Optional Configuration Tasks 1-15

Chapter 2
Administrative Procedures

Managing Your TaskSmart N2400 Appliance 2-1
    Microsoft Management Console 2-3
    Command Prompt 2-7
    LogOff 2-8
    Restart 2-8
    Shutdown 2-9
    Enable Drive A: Boot 2-9
    Readme and Product Information 2-9
    ? (Help) 2-10
Managing Your TaskSmart N2400 Appliance Using a Web Browser 2-11
Power Down and Restart the Appliance 2-12
    Powering Down the TaskSmart N2400 Appliance 2-12
    Restarting the TaskSmart N2400 appliance 2-12
Compaq SANworks Virtual Replicator 2-12
    Storage Pooling 2-13
    Virtual Disks 2-13
    Snapshots 2-13
    Online Volume Growth 2-14
Creating and Scheduling Snapshots 2-15
    Snapshot Overview 2-15
    Creating Snapshots 2-16
    Scheduling Snapshots 2-27
SWVR Lifeguard Service 2-29
    Modify Reserved Pool Space 2-30
Managing Space Usage with Quotas 2-32

Chapter 3
Windows File System Administration

Common Internet File System User and Group Management 3-1
    Domain Compared to Workgroup 3-2
    Managing Users and Groups Effectively 3-2
    Workgroup Environment 3-4
    Domain Environment 3-15
    Windows File System Security 3-55
    Integrating Local File System Security into Windows Domain Environments 3-69
CIFS Shares 3-70
    Setting Up a Share 3-70
    Windows Explorer 3-84
    Administrative Compared to Standard Shares 3-88
    Planning for Compatibility Between CIFS and NFS 3-88

Chapter 4
Integrating UNIX into Windows NT

- Microsoft Services for UNIX 4-1
  - Network File System 4-3
  - Authentication 4-5
  - Server for NFS 4-6
  - User Name Mapping 4-9
  - Mortice Kern Systems Toolkit 4-29
- NFS File Exporting Using SFU 4-29
  - Procedure for NFS Exporting 4-29
  - Testing NFS 4-29
  - Client Groups 4-30
  - File Locking 4-31
  - Auditing 4-32
  - Command Line Capabilities 4-32

Chapter 5
Remote Administration

- Remote Administration 5-1
  - Telnet Server 5-2
  - Remote Shell Daemon 5-3
  - Remote Insight Lights-Out Edition Board 5-4
  - Web User Interface 5-8
  - Compaq Insight Manager 5-9
  - Enterprise Management Applications 5-12
  - Installing the Management Software—On the Client Machine 5-15

Chapter 6
Advanced Administrative Procedures

- Storage Management 6-2
- Drive Arrays and Smart Array Controllers 6-4
  - Array Configuration Utility 6-4
  - Array Controllers 6-6
  - Managing Drive Arrays Using ACU 6-7
  - Creating Logical Drives from Arrays 6-12
- SANworks Virtual Replicator 6-14
  - Creating Pools Using SWVR 6-14
  - Creating Virtual Disks from Pools 6-17
  - Deleting Virtual Disks and Pools 6-19
  - Online Volume Growth 6-21
- Moving Drives 6-26

Advanced Administrative Procedures

continued

Replacing a Failed Drive and Using Spares 6-27
  Hard Drive LED Indicators 6-28
  Replacing Failed Hard Drive Process 6-31
  Using Spare Drives 6-32
  Compromised Fault Tolerance 6-33
Moving Arrays 6-34
Capacity Expansion 6-35
Ethernet Teaming Features and Procedures 6-37
  Compaq Network Teaming and Configuration Utility 6-37
  NIC Teaming Troubleshooting 6-56
Using Uninterruptible Power Supplies 6-58
Password Synchronization 6-59
  Implementation 6-60
  Requirements 6-60
  Password Synchronization—Advanced Settings 6-61
  Installation Procedure 6-62
  Password Synchronization—Default 6-63

Appendix A

Backup Utility Management

Sizing Tools A-2
Developing a Backup Solution A-2
  Types of Tape Solutions A-3
  Tape Device Connection Methods A-3
  Backup Software Vendors A-5
Backup Best Practices A-6

Appendix B

RAID Levels

Distributed Data Guarding B-1
Drive Mirroring B-3

Appendix C
Troubleshooting

Initial Troubleshooting Checklist C-2
Hard Drive Problems C-2
    Hot-Plug Drive Replacement Guidelines C-4
    Unsafe Hot-Plug Drive Replacement Precautions C-5
    Predictive Failure Alert C-6
SCSI Device Problems C-8
TaskSmart N2400 Server Troubleshooting C-8
Software and Firmware Diagnostic Tools C-9
    Default Configuration C-10
    Running Compaq Utilities C-12
    Diagnostics Software C-14
    Array Diagnostic Utility C-18
    Integrated Management Log C-19
    Rapid Error Recovery C-21
    Automatic Server Recovery-2 .... C-22
    ROMPaq Error Recovery Options C-29
    ROMPaq Disaster Recovery C-29
SFU Troubleshooting C-31
Stopping and Starting NFS File Service C-37
Network Interface Controller Troubleshooting C-38
    The NIC Cannot Connect to the Network C-38
    Other Common Network Interface Controller Problems and Solutions C-44
Remote Insight Lights-Out Edition Board Troubleshooting C-46
    Resetting the Remote Insight Lights-Out Edition Board C-46
    Troubleshooting Logon Problems C-47
    Troubleshooting Alert and Trap Problems C-50
    Miscellaneous Remote Insight Lights-Out Edition Board Troubleshooting C-51
QuickRestore C-52
    TaskSmart N2400 Appliance Verification C-52
    QuickRestore Options C-52
    Selecting the Full Menu Option C-53
    QuickRestore Menu Option C-54
    Full Restore Menu Option C-55
    Post QuickRestore and Automated Setup C-56
    Post QuickRestore Additional Setup C-57
Miscellaneous Troubleshooting C-58
    Incorrect ROM C-58
    System Event Log C-58
    External Storage System C-58
    Compaq Insight Manager C-59

Appendix D

Regulatory Compliance Notices

- Regulatory Compliance Identification Numbers D-1
- Federal Communications Commission Notice D-1
  - Class A Equipment D-2
  - Class B Equipment D-2
  - Modifications D-3
  - Cables D-3
- Canadian Notice (Avis Canadien) D-4
  - Class A Equipment D-4
  - Class B Equipment D-4
- Mouse Compliance Statement D-4
- European Union Notice D-5
- Japanese Notice D-5
- Taiwanese Notice D-5
- Laser Devices D-6
  - Laser Safety Warnings D-6
  - Compliance with CDRH Regulations D-6
  - Compliance with International Regulations D-6
  - Laser Product Label D-7
  - Laser Information D-7
- Battery Replacement Notice D-8

Appendix E

Electrostatic Discharge

- Grounding Methods E-2

Index

About This Guide

This guide is designed to be used as a reference for installation, operation, troubleshooting, and future upgrades for the Compaq *TaskSmart*™ N2400 appliance.

Text Conventions

This document uses the following conventions to distinguish elements of text:

Keys	Keys appear in boldface. A plus sign (+) between two keys indicates that they should be pressed simultaneously.
USER INPUT	User input appears in a different typeface and in uppercase.
FILENAMES	File names appear in uppercase italics.
Menu Options, Command Names, Dialog Box Names	These elements appear in initial capital bold letters.
COMMANDS, DIRECTORY NAMES, and DRIVE NAMES	These elements appear in uppercase.
Directory or File Paths	These elements appear in italics.
Type	When you are instructed to *type* information, type the information **without** pressing the **Enter** key.
Enter	When you are instructed to *enter* information, type the information and then press the **Enter** key.

Symbols in Text

These symbols may be found in the text of this guide. They have the following meanings.

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or loss of life.

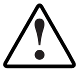
CAUTION: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

IMPORTANT: Text set off in this manner presents clarifying information or specific instructions.

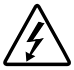
NOTE: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Symbols on Equipment

These symbols may be located on equipment in areas where hazardous conditions may exist.

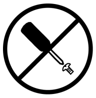


This symbol, in conjunction with any of the following symbols, indicates the presence of a potential hazard. The potential for injury exists if warnings are not observed. Consult your documentation for specific details.



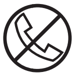
This symbol indicates the presence of hazardous energy circuits or electric shock hazards. Refer all servicing to qualified personnel.

WARNING: To reduce the risk of injury from electric shock hazards, do not open this enclosure. Refer all maintenance, upgrades, and servicing to qualified personnel.



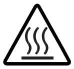
This symbol indicates the presence of electric shock hazards. The area contains no user or field serviceable parts. Do not open for any reason.

WARNING: To reduce the risk of injury from electric shock hazards, do not open this enclosure.



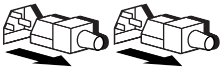
This symbol on an RJ-45 receptacle indicates a network interface connection.

WARNING: To reduce the risk of electric shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.



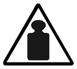
This symbol indicates the presence of a hot surface or hot component. If this surface is contacted, the potential for injury exists.

WARNING: To reduce the risk of injury from a hot component, allow the surface to cool before touching.



These symbols, on power supplies or systems, indicate that the equipment is supplied by multiple sources of power.

WARNING: To reduce the risk of injury from electric shock, remove all power cords to completely disconnect power from the system.



Weight in kg

Weight in lb

This symbol indicates that the component exceeds the recommended weight for one individual to safely handle.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manual material handling.

Important Safety Information

Before installing this product, read the *Important Safety Information* document provided.

Rack Stability

WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- The leveling jacks are extended to the floor.
- The full weight of the rack rests on the leveling jacks.
- The stabilizing feet are secured to the rack if it is a single-rack installation.
- The racks are coupled together in multiple-rack installations.
- Only one component is extended at a time. A rack may become unstable if more than one component is extended for any reason.

Getting Help

If you have a problem and have exhausted the information in this guide, you can get further information and other help in the following locations.

Compaq Technical Support

You are entitled to free hardware technical telephone support for your product for as long you own the product. A technical support specialist will help you diagnose the problem or guide you to the next step in the warranty process.

In North America, call the Compaq Technical Support Phone Center at 1-800-OK-COMPAQ. This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.

Outside North America, call the nearest Compaq Technical Support Phone Center. Telephone numbers for worldwide Technical Support Phone Centers are listed on the Compaq website. Access the Compaq website by logging on to the Internet at

http://www.compaq.com

Be sure to have the following information available before you call Compaq:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages

- Add-on boards or hardware
- Third-party hardware or software
- Operating system type and revision level
- Detailed, specific questions

Compaq Website

The Compaq website has information on this product as well as the latest drivers and flash ROM images. You can access the Compaq website by logging on to the Internet at

http://www.compaq.com

Compaq Authorized Reseller

For the name of your nearest Compaq authorized reseller:

- In the United States, call 1-800-345-1518.
- In Canada, call 1-800-263-5868.
- Elsewhere, see the Compaq website for locations and telephone numbers.

Chapter 1

Initialization

The Compaq *TaskSmart*™ N2400 appliance can be used in many types of computing environments, from basic Microsoft Windows NT workgroups to complicated Windows NT/UNIX multiprotocol domains that rely on domain controllers and Network Information Service (NIS). This chapter provides information about how to initialize the TaskSmart N2400 appliance.

Before completing the tasks in this chapter, verify that both the server and storage enclosure are installed in the rack, and that all cables and cords are connected. It is also necessary to collect certain information required during the initialization process.

Overview

The procedures for setting up your TaskSmart N2400 appliance are outlined in the following sections:

- Preinitialization: Before You Begin
- Task 1: Create the Configuration Data Diskette
- Task 2: Remove the Front Bezel
- Task 3: Insert the Configuration Data Diskette into the Server
- Task 4: Connect the Standard Ethernet Cables
- Task 5: Power Up the Server
- Task 6: Monitor the Initialization Process
- Task 7: Complete the System Configuration

Preinitialization: Before You Begin

Verify That Hardware Installation Is Complete

Before beginning the installation process, verify that the server and storage enclosure are completely installed in the rack and that all cables and cords are connected. A keyboard, monitor, and mouse must also be connected to the server.

IMPORTANT: If you need assistance with rack installation or hardware connections, refer to the Rack Installation and Connection card included in the shipping carton.

Initialization Methods

There are two methods for initializing the TaskSmart N2400 appliance:

- Using the Configuration Utility CD provided with the appliance to create a configuration data diskette
- Using a predetermined configuration data diskette provided by your company

IMPORTANT: If you are using a predetermined data diskette provided by your company, proceed to "Task 2: Remove the Front Bezel" later in this chapter.

Collect Information for Initialization

Collect the general information required to initialize the server for both dynamic host configuration protocols (DHCP) and non-DHCP configurations. You will be asked for this information during initialization. Become familiar with this information before attempting to initialize and configure the server.

Part A: To be completed for DHCP and non-DHCP configurations		
Server Host Name:		
Remote Insight Board Name:	**Remote Insight Board Default User:**	**Password:**
Part B: To be completed for non-DHCP configurations only		
DNS Servers	**IP Address**	
1		
2		
3		
Port*	**IP Address**	
Eth 0		**Subnet Mask**
Eth 1		
Eth 2		
Eth 3		
Eth 4		
Remote Insight Board Eth		
*The TaskSmart N2400 appliance has five Ethernet ports available for network connectivity. It is recommended that the four-port network interface controller (NIC) board be used for file services before using the NIC (Eth 0) port on the system board. Do not configure ports that will not be used. Each Ethernet port must be configured with a separate subnet.		
Note: If NIC teaming is to be implemented, determine which ports will be teamed. Configure these Ethernet ports for DHCP protocol. For more information refer to the Ethernet teaming features and procedures section of Chapter 6, “Advanced Administrative Procedures,” in the administration guide.		
Part C: SNMP Information (optional)		
Trap Destination (IP Address) Manager Client		
Management Traps Community String		
System Management Community String		

Task 1: Create the Configuration Data Diskette

The TaskSmart N2400 appliance includes a Configuration Utility CD that can run on any Windows-based PC. The CD is designed to be graphical and easy-to-use, and to assist you in populating information necessary for initialization.

The following items are required to complete this task:

- Windows-based PC with CD-ROM and diskette drives
- Keyboard, monitor, and mouse
- TaskSmart Configuration Utility CD
- Configuration data diskette

The following steps provide instructions on how to create the configuration data diskette:

1. Power up the Windows-based PC and wait until the operating system has completely loaded.
2. Insert the configuration data diskette into the diskette drive.

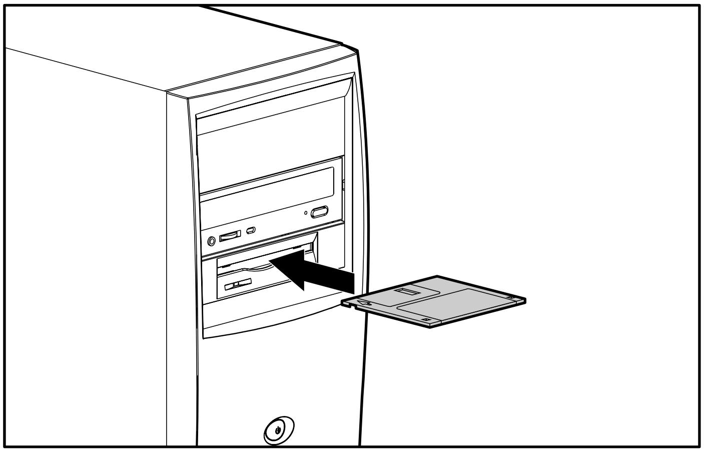


Figure 1-1. Inserting the configuration data diskette into the diskette drive of a PC

3. Insert the Configuration Utility CD into the CD-ROM drive.

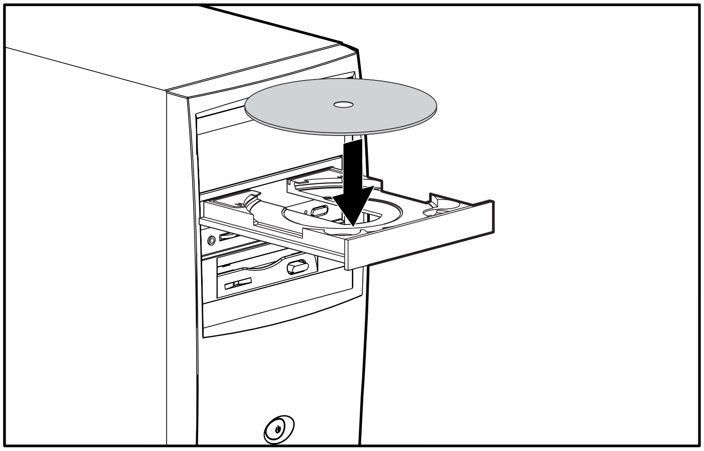


Figure 1-2. Inserting the Configuration Utility CD into the CD-ROM drive of a PC

NOTE: The TaskSmart Configuration Utility CD automatically runs a wizard-style interface that prompts you to enter the appropriate information.

4. The TaskSmart Configuration Utility CD automatically runs a wizard-style interface. To run the interface manually, click **Start,** and then **Run** on the Windows taskbar, and then type the following:

   `{CD ROM drive}:\setup.exe.`

5. Click **N2400** in the Compaq Network Attached Storage Server section.
6. Follow the instructions on the screen to input the correct information.
7. Verify that your information is correct when the Configuration Review screen is displayed.
8. Click the **diskette** icon to save the network information to the configuration data diskette.
9. The Configuration File Output Results screen is displayed when the information is successfully saved to the diskette.
10. Click the **Finish** icon to exit the TaskSmart Configuration Utility.
11. Remove the configuration data diskette and the Configuration Utility CD from the diskette and CD-ROM drives and store in a secure location.

Task 2: Remove the Front Bezel

Figure 1-3 illustrates removing the front bezel from the server:

1. Press the latches on both the left and right sides of the front bezel ❶.
2. Pull the front bezel out, and then upward from the front panel ❷.
3. Remove the STOP! sticker covering the power button on the front bezel.

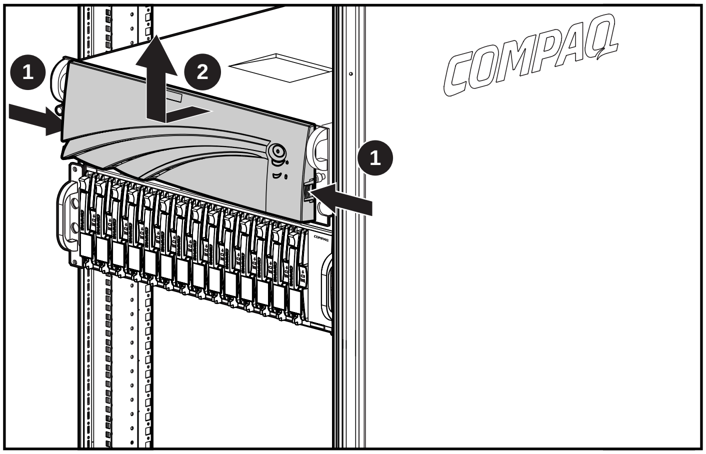


Figure 1-3. Removing the front bezel

Task 3: Insert the Configuration Data Diskette into the Server

Remove the STOP! sticker covering the power button on the front of the server. Insert the configuration data diskette into the diskette drive of the server, as shown in Figure 1-4.

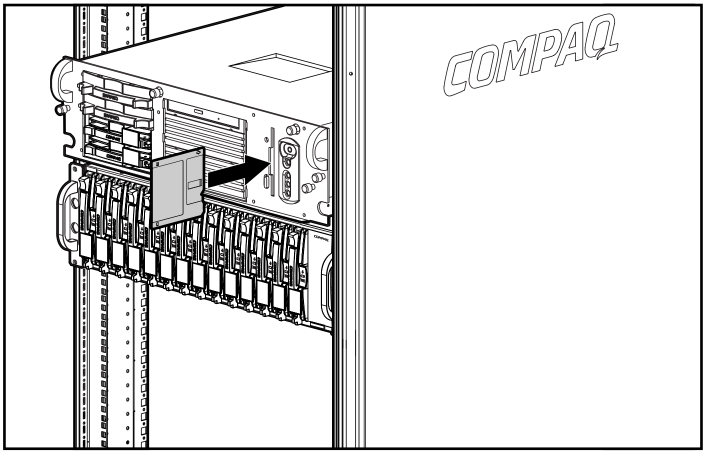


Figure 1-4. Inserting the configuration data diskette into the diskette drive of the appliance

Task 4: Connect the Standard Ethernet Cables

Connect the Ethernet cables to the respective Ethernet connectors in accordance with the information in the “Collect Information for Initialization” section earlier in this chapter. See Figure 1-5 and Table 1-1 for the locations of the Ethernet connectors on the server. Use the four ports (Eth 1 through Eth 4) located on the NIC board before using the Ethernet port (Eth 0) located on the system board.

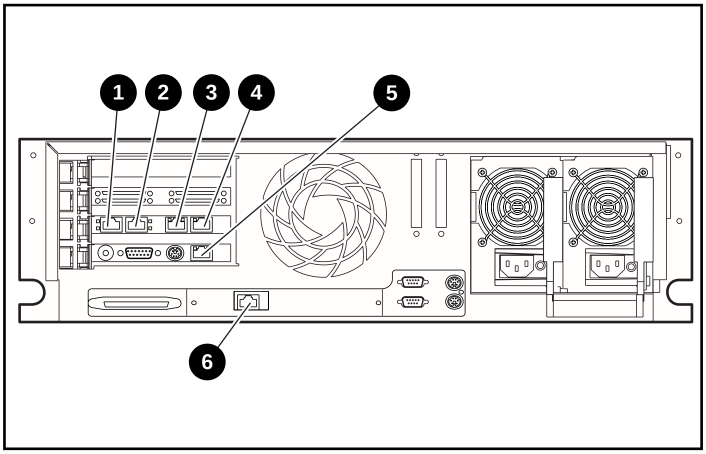


Figure 1-5. Server Ethernet connectors

Table 1-1
Ethernet Network Connectors

Item	Description
❶	NIC Ethernet port 4 (Eth 4)
❷	NIC Ethernet port 3 (Eth 3)
❸	NIC Ethernet port 2 (Eth 2)
❹	NIC Ethernet port 1 (Eth 1)
❺	Remote Insight Lights-Out Edition board Ethernet connector
❻	Ethernet connector (Eth 0) on system board

Note: Connect a loopback cable to any of the server Ethernet ports (Eth 0 through Eth 4) that is not configured for use. Do not connect a loopback cable to the Ethernet ports on the Remote Insight Lights-Out Edition board or the storage enclosure.

Task 5: Power Up the Server

The power button on the TaskSmart N2400 appliance is located on the front panel of the server, as shown in Figure 1-6.

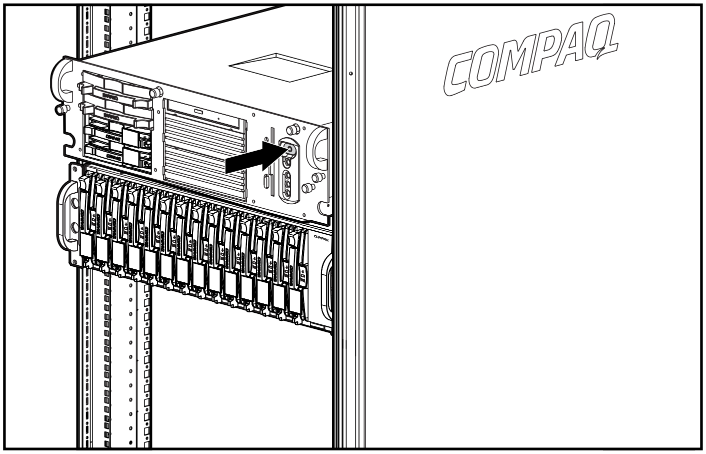


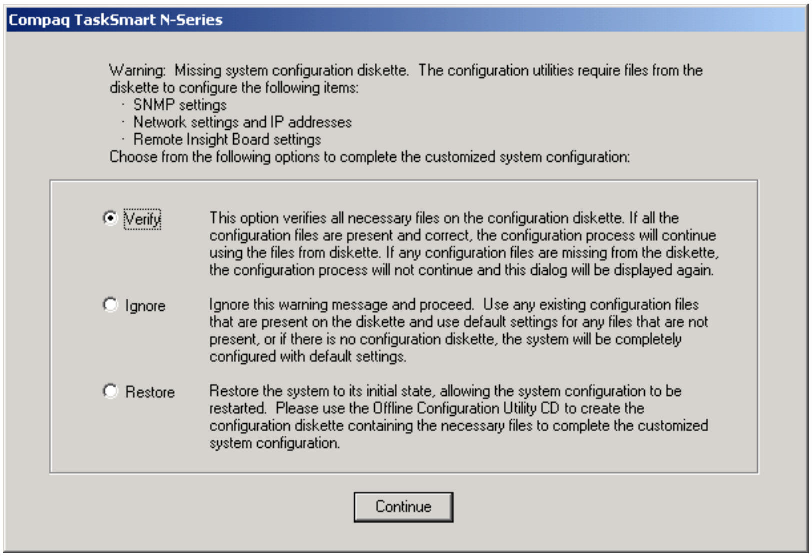
Figure 1-6. Powering up the server

IMPORTANT: Verify that the power LED is green.

Task 6: Monitor the Initialization Process

Once the TaskSmart N2400 appliance is powered up, it automatically completes the initialization process, utilizing the configuration information defined on the configuration data diskette.

If the configuration data diskette is incomplete, or if it is not inserted prior to powering up the server, or if it is inserted at the wrong time, a warning screen is displayed. A warning screen also is displayed if the contents of the configuration data diskette are damaged. Figure 1-7 is an example of one possible warning screen. In all cases, the system administrator must select one of three options, as depicted in Figure 1-7, before initialization can occur.



Warning: Missing system configuration diskette. The configuration utilities require files from the diskette to configure the following items:
- SNMP settings
- Network settings and IP addresses
- Remote Insight Board settings

Choose from the following options to complete the customized system configuration:

● Verify — This option verifies all necessary files on the configuration diskette. If all the configuration files are present and correct, the configuration process will continue using the files from diskette. If any configuration files are missing from the diskette, the configuration process will not continue and this dialog will be displayed again.

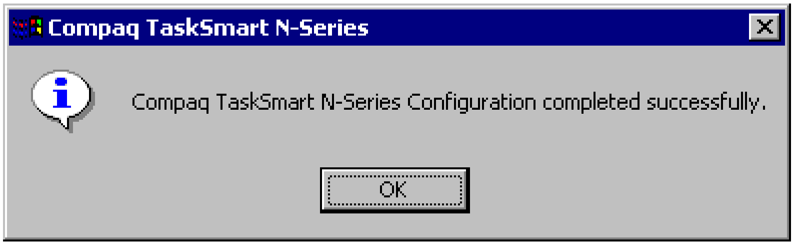
○ Ignore — Ignore this warning message and proceed. Use any existing configuration files that are present on the diskette and use default settings for any files that are not present, or if there is no configuration diskette, the system will be completely configured with default settings.

○ Restore — Restore the system to its initial state, allowing the system configuration to be restarted. Please use the Offline Configuration Utility CD to create the configuration diskette containing the necessary files to complete the customized system configuration.

Figure 1-7. Configuration warning screen

During the initialization process, the system automatically restarts once. Figure 1-8 shows the final screen, which indicates that setup is complete.

CAUTION: To avoid damage to the system configuration, do not interrupt the initialization process once it has begun. The initialization process takes approximately 10 minutes to complete.



Compaq TaskSmart N-Series Configuration completed successfully.

Figure 1-8. Screen illustrating the end of the initialization process

Remove the configuration data diskette from the diskette drive and place it in a secure location with the Configuration Utility CD.

Task 7: Complete the System Configuration

After the initialization process, the next task is to complete the system configuration. Several main configuration utilities specific to the TaskSmart N2400 appliance need adjustment to meet your requirements.

Required Configuration for All Work Environments

Basic configuration of the system date, time, and time zone are required for all work environments.

Changing the Date, Time, and Time Zone

1. Click **Microsoft Management Console.**
2. Expand the **Core Operating System** folder.
3. Double-click the **Control Panel** icon.
4. Double-click the **Date/Time** icon.
5. Click the **Date/Time** tab to view and change the current settings.
6. In the Date area, select the correct month, year, and day.
7. In the box below the date area, use the clock to select the hours, minutes, seconds, or AM/PM indicator.
8. Adjust the selected value by clicking the up or down arrow. Typing directly in the field is often faster than holding down the arrow.
9. Click the **Time Zone** tab to view and change the current settings.
10. In the list box above the map, select the appropriate time zone.
11. If you want your computer clock to automatically adjust when daylight saving time changes, make sure a check mark is displayed in the **Automatically adjust clock for daylight saving changes** box.
12. If changes are made, click **Apply,** and then click **OK.**

Required Configuration by Work Environment

Complete the following configuration tasks based on your specific work environment.

Windows NT Workgroups and Domain Security Environments

- **CIFS share configuration for Windows file access**

  The Common Internet File System (CIFS) shares configuration controls what can connect to the shared drive, based on the user ID and group or groups. This configuration is necessary for Microsoft Windows NT, Microsoft Windows 2000, Microsoft Windows 98, and Microsoft Windows 95 operating system clients.

  For information about CIFS share configuration see “CIFS Shares” in Chapter 3, “Windows File System Administration.”

UNIX and Windows NT Multiprotocol Environments

- **CIFS share configuration for Windows file access**

  The CIFS shares configuration controls what can connect to the shared drive based on the user ID and group or groups. This configuration is necessary for Windows NT, Windows 2000, Windows 98, and Windows 95 operating system clients.

  For information about CIFS share configuration see “CIFS Shares” in Chapter 3, “Windows File System Administration.”

- **User and group mapping configuration**

  When mapping UNIX users to Windows users with Services for UNIX (SFU), the Username Mapping Server maps the group ID (GID) to a Windows NT group using the group mappings, and the mapping server maps the Windows NT user ID to a UNIX user ID. The Access Control List (ACL) determines access, file owner permissions, group owners and permissions, and other user permissions.

  For information about this configuration see “User Name Mapping” in Chapter 4, “Integrating UNIX into Windows NT.”

- **Network File System (NFS) share configuration for UNIX file access**

  NFS is the sharing protocol for UNIX and Linux clients. NFS share permissions are independent of the CIFS share permissions.

  The configuration necessary for NFS sharing can be found in Chapter 4.

Optional Configuration Tasks

The following optional configuration tasks may be completed if default settings are inappropriate for your work environment:

- **Storage management**

  The TaskSmart N2400 appliance is preconfigured at the factory with an efficient storage management layout. However, the default settings can be changed to better represent your company layout.

  Information to reconfigure the storage management layout can be found in the “Storage Management” section of Chapter 6, “Advanced Administrative Procedures.”

- **Snapshot configuration**

  Snapshots are used to immediately recover a lost file or directory, to test a new application against important data without affecting the “real” data, or as the source of data for backups.

  Information for the configuration of snapshots can be found in “Creating and Scheduling Snapshots” in Chapter 2, “Administrative Procedures.”

- **Remote management software installation and configuration**

  The TaskSmart N2400 appliance can be remotely administered. System monitoring applications allow the administrator to accomplish normal administrative tasks from any remote location using a Web browser.

  Installation and configuration information can be found in the “Remote Administration” section of Chapter 5, “Remote Administration.”

- **Tape backup software installation and configuration**

  Backup software is a necessary component for any work environment. For recommended best practices and suggested software, see Appendix A, “Backup Utility Management.”

- **Password synchronization for UNIX and Windows NT in multiprotocol environments only**

  Password synchronization is an optional service that synchronizes Windows NT passwords with UNIX passwords using the Windows NT platform as the source of the passwords.

  To configure this optional service for your work environment see “Password Synchronization” in Chapter 6.

Chapter 2

Administrative Procedures

The Compaq TaskSmart N2400 appliance is an engineered solution for file serving in multiprotocol environments. The TaskSmart N2400 console can be accessed remotely through the Remote Insight Lights-Out Edition board or directly using an installed keyboard, monitor, and mouse (KMM). This chapter discusses the administrative procedures for daily maintenance of your work environment. A Web-based user interface is also available for administrative tasks. This interface contains detailed online help files documenting its features.

These procedures include:

- Managing Your TaskSmart N2400 Appliance
- Managing Your TaskSmart N2400 Appliance Using a Web Browser
- Power Down and Restart the Appliance
- Compaq *SANworks*™ Virtual Replicator (SWVR)
- Creating and Scheduling Snapshots
- SWVR Lifeguard Service
- Managing Space Usage with Quotas

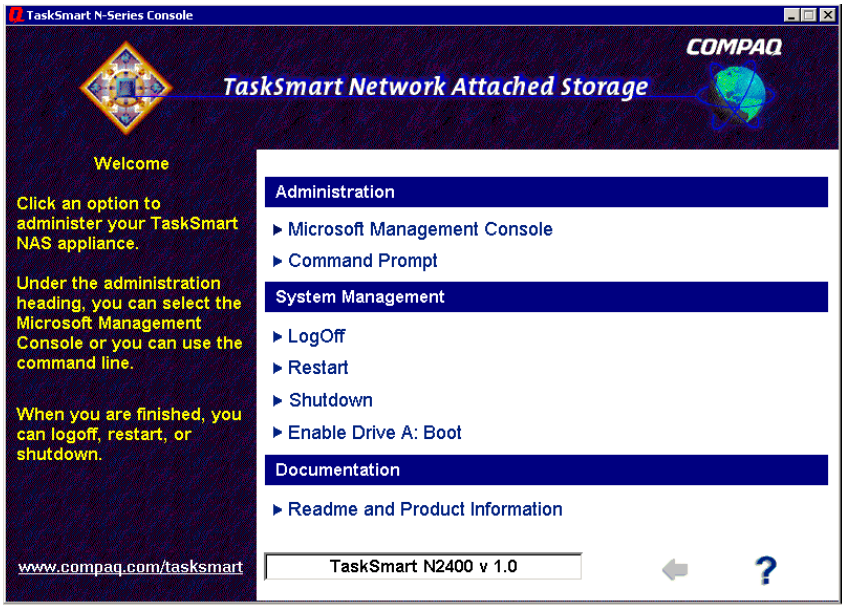
Managing Your TaskSmart N2400 Appliance

The TaskSmart N2400 appliance has been designed with ease of management in mind. For this reason, a special management console has been created to provide links to all major administrative tasks. This console, specific to the TaskSmart N2400 appliance is designed to make management easier and more intuitive by reducing the usual Windows desktop to show only those items required for network attached storage (NAS) administration.

After logging on to the system, a menu listing the following tasks is displayed:

- Microsoft Management Console
- Command Prompt
- LogOff
- Restart
- Shutdown
- Enable Drive A: Boot
- Readme and Product Information
- ? (Help)

The TaskSmart N2400 console is a framework and launching pad for the various management tasks specific to the TaskSmart N2400 appliance. The TaskSmart N2400 console includes several options, as shown in Figure 2-1.



TaskSmart N-Series Console
COMPAQ
TaskSmart Network Attached Storage

Welcome

Click an option to administer your TaskSmart NAS appliance.

Under the administration heading, you can select the Microsoft Management Console or you can use the command line.

When you are finished, you can logoff, restart, or shutdown.

Figure 2-1. TaskSmart N2400 Console

Microsoft Management Console

From the TaskSmart N2400 console, click **Microsoft Management Console** to launch the Microsoft Management Console (MMC), an application that is specifically tailored to the TaskSmart N2400 appliance.

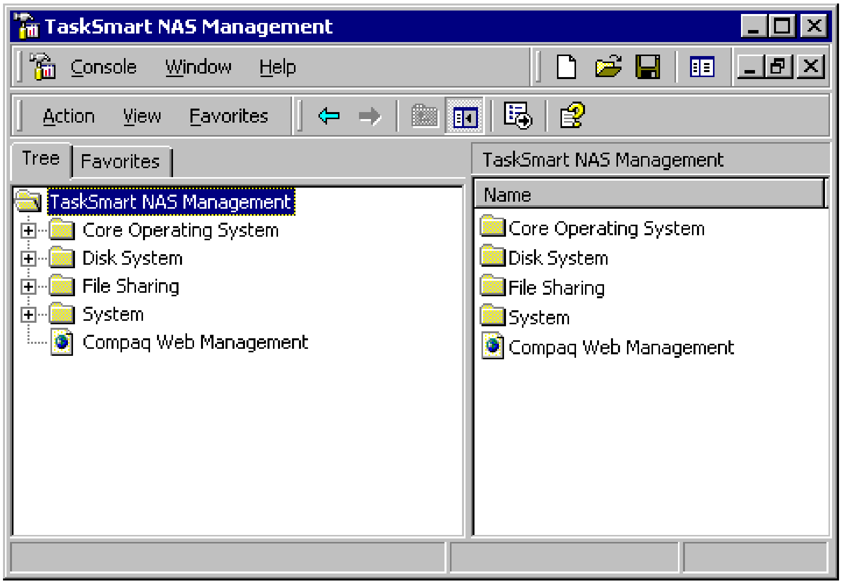


Figure 2-2. Microsoft Management Console (MMC) screen

The MMC maintains the graphical user interface (GUI) for all administrative tasks and is divided into the following four major sections.

Core Operating System

The Core Operating System folder contains MMC snap-ins that configure the core Windows 2000 operating system. A snap-in is a software component that is the smallest unit of a console. One snap-in represents one unit of management behavior. The MMC snap-ins include:

- Certificates for the Local Computer
- Event Viewer
- Internet Information Services
- IP Security Policies on the Local Machine
- Local Computer Policy
- Local Users and Groups
- Performance Logs and Alerts
- Security Configuration, Analysis, and Templates
- Services
- System Monitor
- Control Panel

Disk System

The Disk System folder contains MMC snap-ins that configure the disk system.

The MMC snap-ins include:

- Compaq Array Configuration Utility
- Snapshot Manager

File Sharing

The File Sharing folder contains MMC snap-ins for configuration of exports. The snap-ins include:

- Shared Folders
    - Shares
    - Sessions
    - Open Files
- Service for UNIX (SFU)
    - Refresh NFS Server
    - Server for NFS
    - Telnet Server
    - User Name Mapping
    - Password Synchronization

System

The System folder contains MMC snap-ins that configure the hardware system. The snap-ins include:

- Device Manager
- System Information

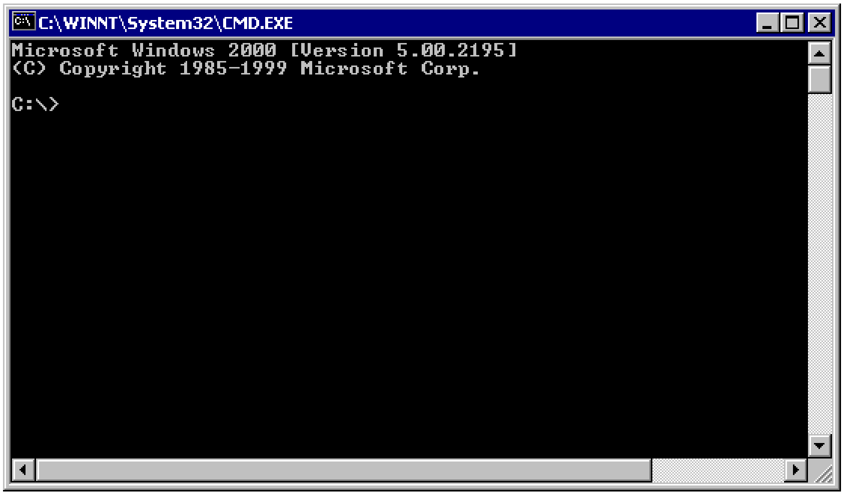
Compaq Web Management

The Compaq Web Management folder contains Web-based administration tools for the TaskSmart N2400 appliance. These tools include:

- Web-Based Administrative Methods
  - Compaq Web-Based Enterprise Management
  - Compaq Management Agents
- Native Administrative Methods
  - Windows 2000 Administrative Tools
  - Compaq System Tools
  - Compaq SWVR Management
  - Services for UNIX Management
  - Other Tools
  - Third-Party Tools

Command Prompt

Clicking the **Command Prompt** button launches a command interpreter for running command line programs and utilities. The usual Windows 2000 command line utilities can be used here, such as net view, net use, net stop, ipconfig, ping, and cd. Additionally, many of the appliance software components, including Microsoft Services for UNIX, have complete command-line interfaces that may be accessed from the command prompt. Check the specific software component documentation and the Windows Powered OS help for more details about command line utilities.



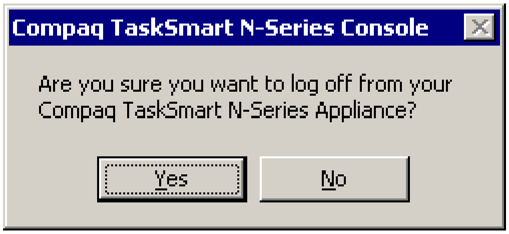
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>
```

Figure 2-3. Command Prompt screen

LogOff

Clicking the **LogOff** option launches a dialog box that asks if you wish to log off the system. Answering yes logs the current user off and prepares the system for someone else to log on.


Compaq TaskSmart N-Series Console

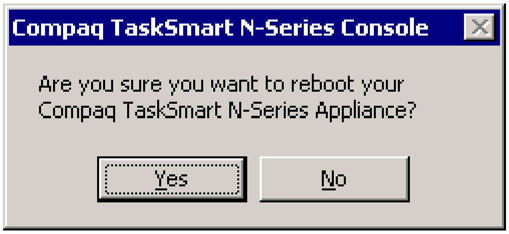
Are you sure you want to log off from your Compaq TaskSmart N-Series Appliance?

Figure 2-4. Logoff dialog box

Restart

Clicking the **Restart** option launches a dialog box that asks if you wish to reboot the system. If the response is yes, the system is restarted, as long as the user logged on has appropriate privileges. The button is disabled if a user is not authorized to restart the system.

> **NOTE:** Before restarting or powering down the system, make file server users aware of service interruption. This warning gives them the opportunity to save their work and exit the files that are open.

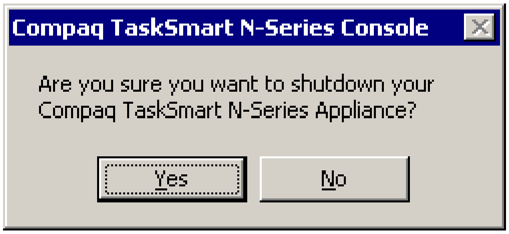

Compaq TaskSmart N-Series Console

Are you sure you want to reboot your Compaq TaskSmart N-Series Appliance?

Figure 2-5. Restart system dialog box

Shutdown

The **Shutdown** option launches a dialog box that asks if you wish to shut down the system. If the response is yes, the system is halted gracefully. The **Shutdown** option is disabled if the user is not authorized to restart the system.



Are you sure you want to shutdown your Compaq TaskSmart N-Series Appliance?

Figure 2-6. Shutdown dialog box

Enable Drive A: Boot

The **Enable Drive A: Boot** option allows you to enable the diskette drive as a boot drive.

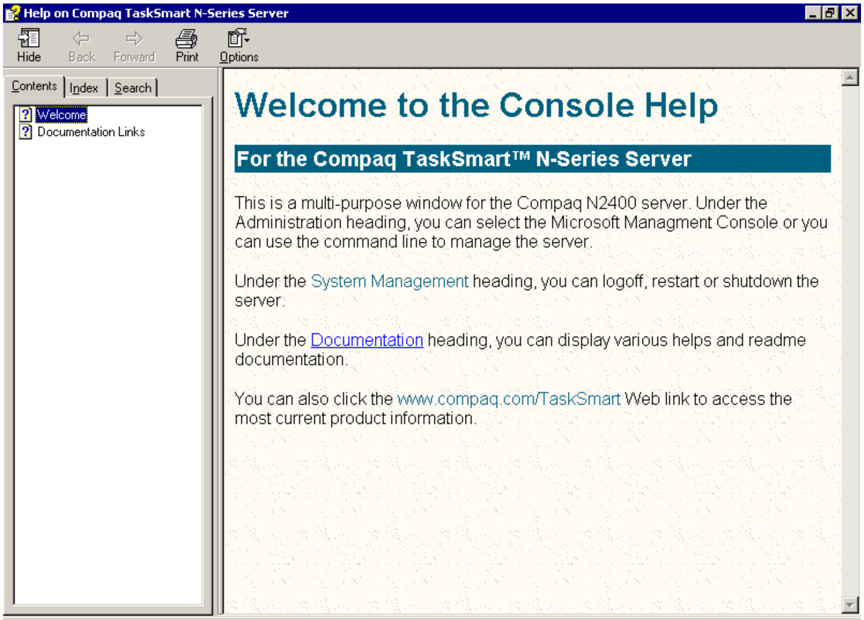
Readme and Product Information

The **Readme and Product Information** option allows you to access the readme and product information files. A dialog box is displayed that lists the software components of the appliance. The following is a list of the available components:

- Array Configuration Utility Help
- Compaq Management Agents Readme
- Core Operating System Help
- Quota Help
- Services for UNIX Help
- TaskSmart N2400 Release Notes
- Virtual Replicator Help
- Web Server Help

? (Help)

Clicking the **? (help)** icon launches the online help files for each component.



Welcome to the Console Help

For the Compaq TaskSmart™ N-Series Server

This is a multi-purpose window for the Compaq N2400 server. Under the Administration heading, you can select the Microsoft Managment Console or you can use the command line to manage the server.

Under the System Management heading, you can logoff, restart or shutdown the server.

Under the Documentation heading, you can display various helps and readme documentation.

You can also click the www.compaq.com/TaskSmart Web link to access the most current product information.

Figure 2-7. Help dialog box

Additional Help

If additional help is required beyond the scope of this document, refer to the Documentation CD to locate the following resource documentation:

- *SANworks™ Virtual Replicator Administration Guide*
- *Remote Insight Lights-Out Edition Board User Guide*
- *Smart Array 5300 User Guide*
- *Fast Ethernet and Gigabit NIC User Guide*
- *Server Online Reference Guide*

For additional help, refer to the following resources:

- MMC Help button
- URL www.compaq.com/Tasksmart

Managing Your TaskSmart N2400 Appliance Using a Web Browser

The TaskSmart N2400 appliance includes a Web-based user interface for the administrator to remotely manage the machine. The Web-based user interface provides user and group management, share management, SANworks Virtual Replicator management, and a subset of MicrosoftWindows 2000 operations. In addition, the Web-based user interface includes wizards to guide the administrator while performing repetitive tasks, for example, creating a share. To access the Web-based user interface, launch a Web browser and enter http://<*your TaskSmart machine name or IP address*>:3201/ in the address field. Online help for the Web interface is available.

Power Down and Restart the Appliance

Powering Down the TaskSmart N2400 Appliance

1. From the TaskSmart N2400 console, click **Shutdown**.
2. After the power-down sequence is complete, press the power button located on the server. The indicator light is amber when the appliance is properly powered down.

IMPORTANT: Notifying users before powering down the system is recommended. Both UNIX and Windows NT users can be drastically affected if they are not prepared for a system power-down.

Restarting the TaskSmart N2400 appliance

1. From the TaskSmart N2400 console, click **Restart.**
2. Follow the instructions as they are displayed on the screen.

Compaq SANworks Virtual Replicator

Compaq SANworks Virtual Replicator (SWVR) provides advanced, centralized storage management capabilities in Microsoft Windows NT and Windows 2000 computing environments. Innovative storage management features simplify storage configuration and management, and enhance availability and scalability.

SWVR gives you manageable storage tools:

- **Pools—**form storage units from hardware arrays or physical drives
- **Virtual disks—**divide pool space of any size, up to 2 terabytes
- **Snapshots—**make instant copies of the virtual disks
- **Online volume growth—**increase the size of the virtual disk

Storage Pooling

SWVR enables the grouping of hardware array storage, or physical drives, into a logically proportioned pool of drive space. You can create any number of pools, using industry-standard storage components and controller-based, fault-tolerant drive arrays (such as SANworks RAID arrays). The logical drives created from the RAID arrays are referred to as storage units. The storage units provide drive space for the pool in the same way that physical drives provide drive space for a SANworks RAID array.

Virtual Disks

SWVR controls how data is stored on a virtual disk. The virtual disks perform and behave in exactly the same way as physical drives do. You can format and map drive letters to them, and read from and write to them. Disk virtualization allows you to optimally tailor drive space to the size required by users and their applications. You can make the sizes of the virtual disks match the requirements of your applications and users. For example, if a user needs 650 MB of drive space, you can create a 650-MB virtual disk. If you have a terabyte database, you can combine several drives or SANworks RAID arrays into a single pool and create a 1-terabyte virtual disk that spans that physical storage. The size of the virtual disks that you create can range from 10 MB to 1 terabyte, depending on free pool space and other limits set at the time of pool creation. The TaskSmart N2400 appliance has a maximum storage capacity of 2 terabytes, which can consist of up to two 1-terabyte virtual disks. See Chapter 6, “Advanced Administrative Procedures,” for more information about virtual disks.

Snapshots

SWVR lets you make instant replicas, called snapshots, of virtual disks in a matter of seconds. Snapshots enable the instant creation of multipurpose virtual replicas of production data without having to physically copy the data. Snapshots function in exactly the same way as ordinary physical drives with read and write capabilities do. Snapshots should be considered temporary in nature. See the “Creating and Scheduling Snapshots” section later in this chapter for additional information.

Online Volume Growth

SWVR provides the ability to increase storage capacity without disrupting operations on Windows 2000 systems. Normally, when you grow a RAID set, the operating system does not recognize the size change until you restart the system. The SWVR online volume growth feature directs the operating system to update the size of a physical drive or virtual disk without requiring a system restart. Online volume growth also can instruct the operating system to grow the on-disk partition information for a volume. This feature allows a volume to grow into unused space made available by either increasing the size of a drive or by deleting one or more adjacent partitions. With online volume growth, you can easily increase storage capacity as required by your users and applications, and do it with zero downtime.

The online volume growth feature operates only on basic and virtual disks formatted with the New Technology File System (NTFS). It does not work with dynamic drives. Chapter 6 provides additional information about SWVR.

Creating and Scheduling Snapshots

Snapshot Overview

Snapshots are copies of the data that is saved on virtual disks. Snapshots initially take up very little space on the hard drive and can be created in mere seconds. Snapshots are extremely beneficial. They can be used to immediately recover a lost file or directory, to test a new application with important data without affecting the “real” data, and as a source of data for backups. Snapshots are a temporary backup of your data and are not meant to be a permanent form of the data.

Snapshots work by mapping blocks of virtual disks and intercepting virtual disk writes. Each initial write to a data block on the virtual disk causes that write to perform a copy of the original data before replacing it with the new data being written. This action is known as a copy-out and preserves a copy of the virtual disk as it was when the snapshot was created. The copy is available until the snapshot is deleted.

When using snapshots, performance of the virtual disk may be affected, depending on the rate that your data is changing and the number of snapshots kept for each virtual disk. Read performance of the virtual disk remains constant, regardless of the presence of snapshots. Read performance of the snapshot is identical to that of the virtual disk. Write performance, however, may vary. Each initial write to a virtual disk area causes a copy-out to the snapshot, and the initial write is slower than if a snapshot is not being used. Copy-out is not performed on subsequent writes to the same virtual disk block, so write performance is unaffected after the initial write to each block.

Predicting the exact effect of snapshots on any particular virtual disk is difficult, because several variables are involved. These variables include the type of applications accessing the data and the rate of change of the files on the virtual disk. When a high percentage of writes is made to the same area, as when a file is constantly rewritten, the area is called write locality. Virtual disks with high write locality experience less performance degradation due to snapshots.

Snapshot Facts:

- Snapshots are created on a per-virtual disk basis.
- You can create up to 12 snapshots per virtual disk.
- You can create snapshots of snapshots.
- Snapshots can be read-only or read-write.
- Snapshots must be assigned to a drive letter to be accessible.
- Snapshots can be shared in the same manner as virtual disks.
- Snapshots are meant to be temporary in nature.
- Snapshots are automatically deleted if pool space becomes critical.

Creating Snapshots

Snapshots are a daily maintenance tool for your TaskSmart N2400 appliance. Before creating a snapshot, the TaskSmart N2400 appliance must have a pool, or pools, of space and one or more virtual disks established. The TaskSmart N2400 appliance comes preconfigured with pools and virtual disks. Verify that there is adequate free pool space to support snapshots.

IMPORTANT: Snapshots are temporary in nature and are automatically deleted by the system if free pool space becomes critical. Snapshot data loss can occur. See “SWVR Lifeguard Service” later in this chapter for more information.

Chapter 6 provides instructions for altering the preconfigured snapshot layout for your work environment. Instructions also include the procedures required to create pools and virtual disks.

After the pool or pools of space and one or more virtual disks are established, the process to create snapshots can begin.

1. From the TaskSmart N2400 console, click **Microsoft Management Console,** and then click **Disk System.**
2. Click **Snapshot Manager**. Then select and click the desired pool.

3. Select a virtual disk.

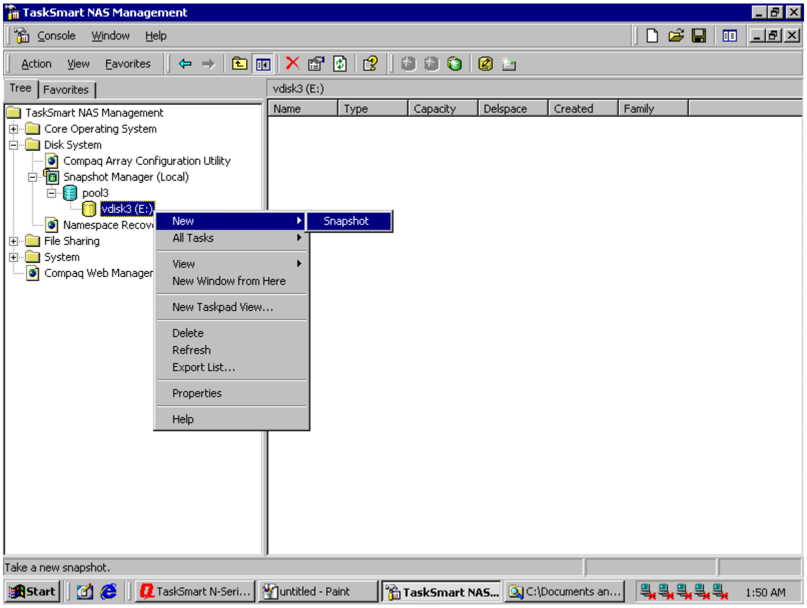
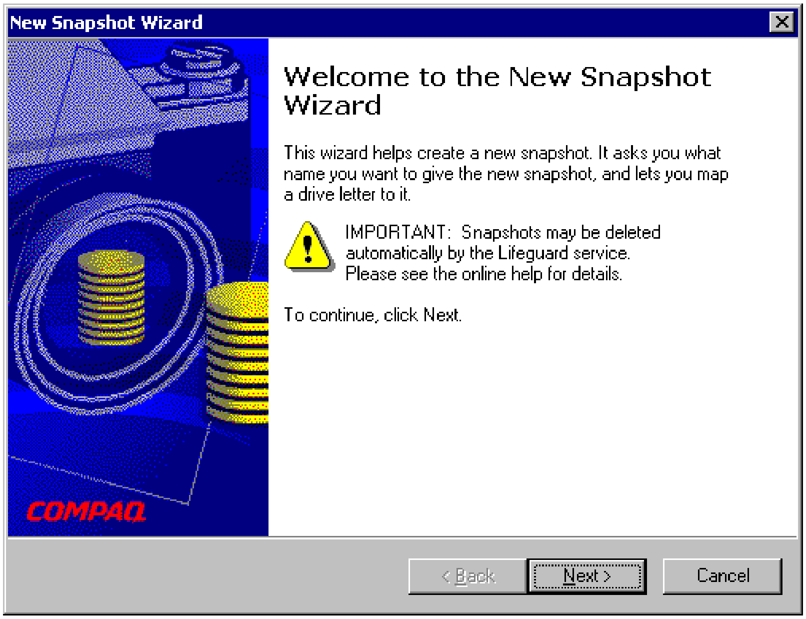


Figure 2-8. Snapshot Manager screen, creating snapshots

4. Right-click the virtual disk, click **New,** and then click **Snapshot.** The Snapshot Wizard opens and leads you through a series of questions.



Welcome to the New Snapshot Wizard

This wizard helps create a new snapshot. It asks you what name you want to give the new snapshot, and lets you map a drive letter to it.

IMPORTANT: Snapshots may be deleted automatically by the Lifeguard service. Please see the online help for details.

To continue, click Next.

Figure 2-9. New Snapshot Wizard screen

5. Click **Next.** The Snapshot Information screen is displayed.
6. Enter a name for the snapshot.

NOTE: Appropriate snapshot naming and volume naming must be used to identify each snapshot individually.

7. Click **Next.** The Drive Letter Assignment screen is displayed.
8. Click **Map Drive Letter** and select a drive letter. Enter a volume label. The default is the same volume label as the virtual disk. Optionally, click **No Drive Letter.**

NOTE: It is not necessary to assign a drive letter to the snapshot until you need access to the snapshot. However, if you plan to create one snapshot per virtual disk, it is advisable to assign a drive letter at this time.

9. Click **Next.**
10. Click **Finish.**

Snapshot Access

- Snapshots can be read-write, and if they are shared, users can access a snapshot and edit the data. If snapshots are shared with write access enabled, it is recommended that a snapshot of the original snapshot be created. There is no backup of the original snapshot unless a snapshot of it is taken. By controlling the share permissions, administrators can make snapshots read-only as an alternative to creating snapshots of snapshots.

  NOTE: Snapshots of snapshots can impede performance when both snapshots are running on the same virtual disk.

- The parent-child relationship of snapshots of snapshots is not maintained on the server. Appropriate snapshot naming and volume naming must be used to identify each snapshot individually. For example:
  - Name the parent “Snapshot A”
  - Name the child “Child of Snapshot A”

Snapshots and Backup

Because snapshots are quick to create, it is possible to capture a coherent view of the virtual disk data with little or no application downtime. Lack of application downtime removes the traditional backup window or the amount of time taken to back up to offline media. While many applications must be shut down to capture an accurate backup, snapshots capture a point-in-time view of the data that can be used as the source of backup data. Applications can continue processing against the virtual disk data. Therefore, applications may only have to be interrupted for a few seconds during the snapshot process.

CAUTION: Snapshots are not a replacement for reliable, periodic data backup. If free pool space becomes critical, snapshots can be automatically deleted. See “SWVR Lifeguard Service” later in this chapter. Also, snapshots are a short-term convenience and reside on the same physical drives as the data. If something happens to the data drives, the snapshots are also affected. Read Appendix A, “Backup Utility Management,” for suggestions on how to back up your TaskSmart N2400 appliance.

Snapshots, Restoring Files, and Directories

Snapshots may be used as a highly efficient way to maintain online backups of a virtual disk, enabling immediate file and directory recovery. Snapshots are assigned to a drive letter and used exactly like virtual disks. If a file or directory is lost or corrupted, it can be recovered easily. The user can switch to the snapshot drive and copy the file or directory back to its original location on the virtual disk or an alternate location.

IMPORTANT: To preserve the integrity of a point-in-time snapshot of your virtual disk, ensure that it is exported as read-only.

Snapshots and Restoring a Virtual Disk

When data on a virtual disk becomes corrupted, restore the virtual disk from your normal tape backup. Alternatively, use an existing and valid snapshot of the virtual disk to restore the entire virtual disk from the existing snapshot.

NOTE: Snapshots are not a replacement for normal tape backup.

CAUTION: Snapshot recovery causes temporary pool space consumption because of the need to preallocate pool space for the newly recovered virtual disk. There must be sufficient free pool space; otherwise, a pool-full condition may occur and Lifeguard may delete the snapshot from which you are restoring. If your only snapshot is deleted, you must restore from tape backup. See “SWVR Lifeguard Service” later in this chapter.

The Restore From Snapshot Wizard schedules the re-creation of a virtual disk from a snapshot. If specified, upon successful completion of the schedule, the previous virtual disk and snapshot are both deleted. Perform the following steps:

1. Remove all shares associated with the virtual disk that you are intending to restore.
2. Delete all snapshots of the virtual disk that you are intending to recover, except for the snapshot that will be used for the recovery. Additionally, to free up pool space, delete any unnecessary snapshots of other virtual disks in the same pool.

3. Make sure that you have enough free pool space to accomplish the recovery, and if necessary, add logical disks to increase pool free space.

   Typically, you need pool free space equivalent to the current size of the virtual disk that you are recovering, plus the space currently used by the snapshot that you will use for the recovery. To determine the amount of space used by this snapshot, access the Snapshot Manager, and then click the virtual disk listing. Locate the snapshot name in the right pane. The amount of the space used by the snapshot is in the **Delspace** column.

4. From the TaskSmart console:

   a. Click **Microsoft Management Console.**

   b. Click **Disk System.**

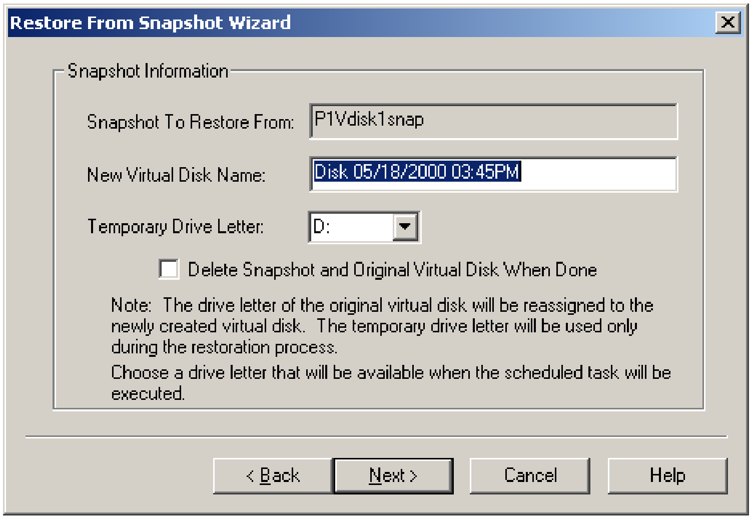
   c. Click **Snapshot Manager.** Expand the list to show Pools, Virtual Disks, and Snapshots.

   d. Right-click the listing for the appropriate snapshot to restore from. Select **All Tasks, Scheduled Tasks Online Restore from a Snapshot.**

e. The Restore From Snapshot Wizard launches. On the opening screen, click **Next.**

f. If desired, enter a new Virtual Diskname and Drive Letter. Check **Delete Snapshot and Original Virtual Disk When Done.**

g. Click **Next**.



Snapshot To Restore From: P1Vdisk1snap

New Virtual Disk Name: Disk 05/18/2000 03:45PM

Temporary Drive Letter: D:

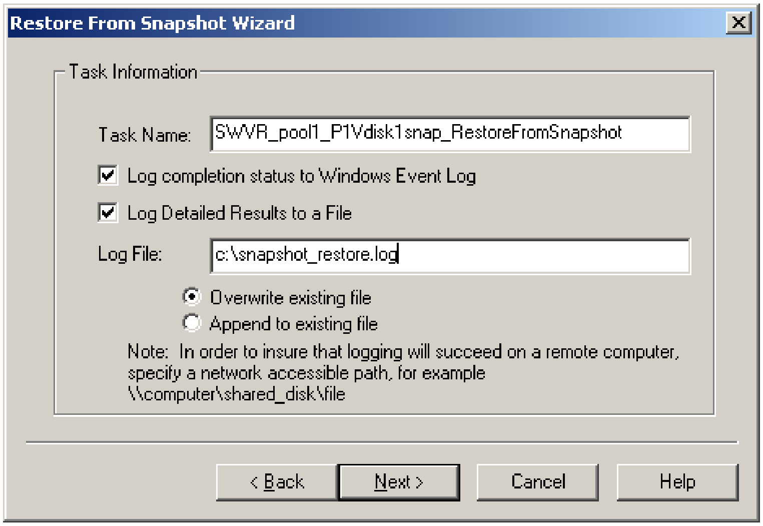
☐ Delete Snapshot and Original Virtual Disk When Done

Note: The drive letter of the original virtual disk will be reassigned to the newly created virtual disk. The temporary drive letter will be used only during the restoration process.
Choose a drive letter that will be available when the scheduled task will be executed.

Figure 2-10. Restore From Snapshot Wizard, Snapshot Information dialog box

h. Select **Log completion status to Windows Event Log** and **Log Detailed Reports to a File.** Then, enter a Log File path\filename, and click **Overwrite existing file.**

i. Click **Next.**



Task Name: SWVR_pool1_P1Vdisk1snap_RestoreFromSnapshot

☑ Log completion status to Windows Event Log

☑ Log Detailed Results to a File

Log File: c:\snapshot_restore.log

● Overwrite existing file

○ Append to existing file

Note: In order to insure that logging will succeed on a remote computer, specify a network accessible path, for example \\computer\shared_disk\file

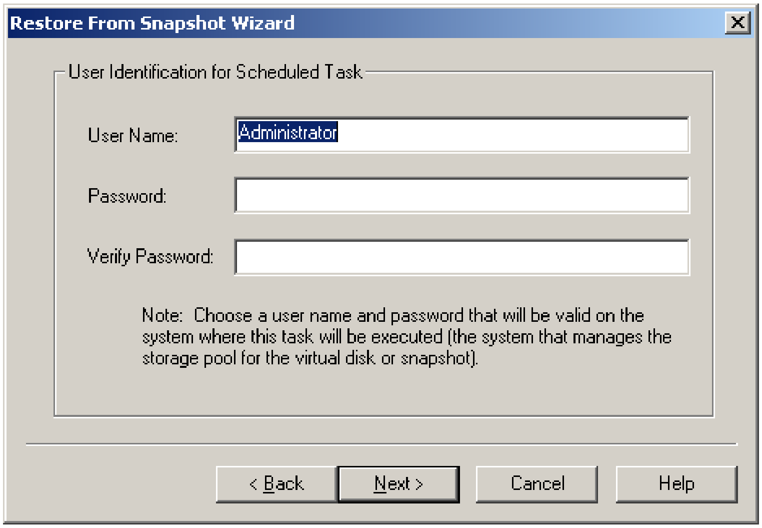
Figure 2-11. Restore From Snapshot Wizard, Task Information dialog box

---

IMPORTANT: Complete the following step to have a record of the transaction.

---

j. Enter User Name, Password, and Verify Password. Click **Next.**



Restore From Snapshot Wizard

User Identification for Scheduled Task

User Name: Administrator

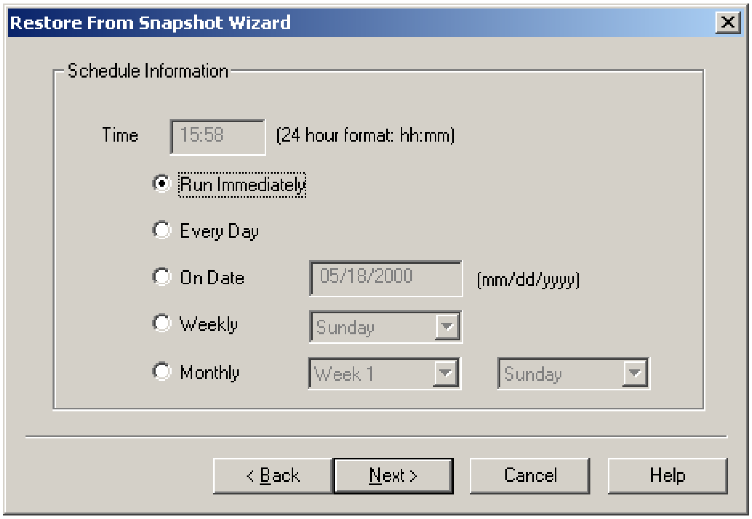
Password:

Verify Password:

Note: Choose a user name and password that will be valid on the system where this task will be executed (the system that manages the storage pool for the virtual disk or snapshot).

Figure 2-12. Restore From Snapshot Wizard, User Identification for Scheduled Task dialog box

k. Enter Schedule Information. Select **Run Immediately** or specify when you want the restore to run. Click **Next.**



Restore From Snapshot Wizard

Schedule Information

Time: 15:58 (24 hour format: hh:mm)

● Run Immediately

○ Every Day

○ On Date: 05/18/2000 (mm/dd/yyyy)

○ Weekly: Sunday

○ Monthly: Week 1, Sunday

Figure 2-13. Restore From Snapshot Wizard, Schedule Information dialog box

5. Click **Next,** and then click **Finish.**

Pool Sizing and Snapshots

When initially implementing snapshots, the first priority is to gain an understanding of the amount of additional pool space required by the snapshots. As previously described, this assessment is a function of the write activity, its locality, the projected lifetime of the snapshot, and the number of snapshots per virtual disk. By default, 30 percent of the pool is reserved for snapshots

SWVR includes a Snapshot Planner utility. The Snapshot Planner utility must be installed and run only on existing servers. The utility must not be run on the TaskSmart N2400 appliance. The Snapshot Planner monitors all write activity to a selected volume and reports the amount of pool space that a snapshot of the volume consumes. The Snapshot Planner provides complete pool and volume sizing information. The size of the virtual disks and the size of the pool are equally important.

Snapshots and Drive Defragmentation

CAUTION: Defragmentation must not be performed when snapshots exist, because defragmenting a virtual disk rewrites its files on the virtual disk. If you must defragment, first delete the snapshots.

A drive defragmenter attempts to consolidate files on a drive by reading various parts of the files and rewriting them to become contiguous on the drive. Contiguous files increase drive performance. When virtual disks are created from the drive space pool, the software attempts to make them as contiguous as possible on the underlying storage units (logical drives and arrays).

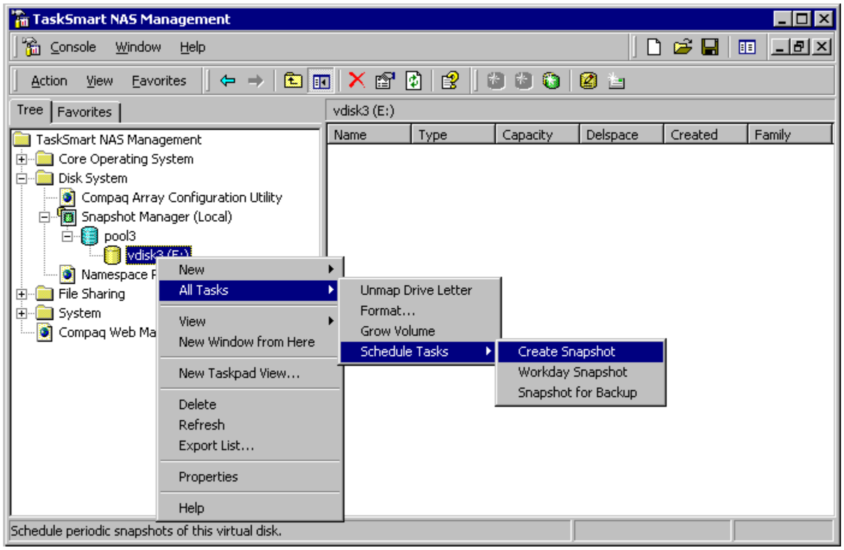
IMPORTANT: Defragmenting a virtual disk is appropriate when snapshots are not present. However, the Windows 2000 operating system native defragmenter does not work on SWVR virtual disks and must be avoided.

IMPORTANT: Drive defragmentation only operates on virtual disks formatted with a 4-KB or smaller cluster size.

Scheduling Snapshots

Snapshots can be scheduled for each virtual disk at any arbitrary or regularly occurring date and time. The steps below outline the snapshot scheduling process.

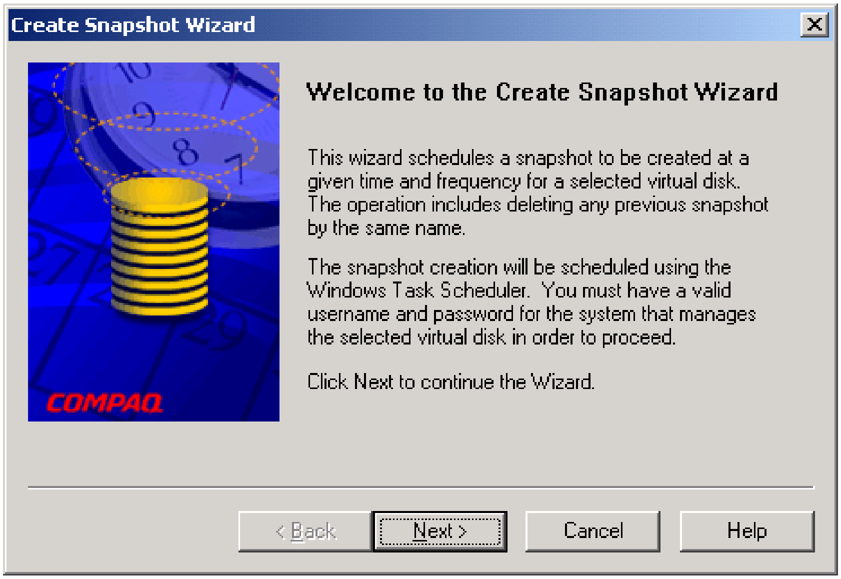
1. From the TaskSmart console, click **Microsoft Management Console,** and then click **Disk System.**
2. Click **Snapshot Manager,** and then select a pool.
3. Right-click a selected virtual disk.
4. Click **All Tasks,** then click **Schedule Tasks,** and then click **Create Snapshot.**



Schedule periodic snapshots of this virtual disk.

Figure 2-14. Snapshot Manager screen, scheduling snapshots

5. The Create Snapshot Wizard launches. Click **Next.**



Welcome to the Create Snapshot Wizard

This wizard schedules a snapshot to be created at a given time and frequency for a selected virtual disk. The operation includes deleting any previous snapshot by the same name.

The snapshot creation will be scheduled using the Windows Task Scheduler. You must have a valid username and password for the system that manages the selected virtual disk in order to proceed.

Click Next to continue the Wizard.

Figure 2-15. Create Snapshot Wizard screen

6. Configure each screen of the wizard with your data.
7. Select **Finish** when the last screen is complete.
8. To confirm the scheduled task:
   a. Right-click **Virtual Disk.**
   b. Select **Properties.**
   c. Select the **Scheduled Task** tab. View the task listing for the task name and scheduled date/time.
   d. Click **OK.**

Recurring snapshot tasks can be configured so that a snapshot runs a backup command and automatically deletes itself when the backup is complete.

IMPORTANT: Veritas Backup Exec does not allow snapshots to run a backup command and to automatically delete themselves when the backup completes.

SWVR Lifeguard Service

SWVR Lifeguard is a utility that watches storage pools for pool-full conditions and deletes snapshots when a pool is nearly full. Pool-full conditions cause writes to the drive to be delayed. These conditions can occur when snapshots are being used and insufficient space is left in the pool to allow copying the data from the original virtual disk to the snapshot. If this situation occurs, the system delays the write to both the original virtual disk and the snapshot.

CAUTION: If the pool is improperly sized and there is an insufficient amount of free space in the pool, Lifeguard automatically deletes the oldest snapshots. This action prevents a critical space deficit that could delay or lose writes.

Because snapshots utilize free space in the pool, a pool-full condition can be a result of poor or improper pool space planning. Make sure there is sufficient space for snapshots. By default, 30 percent of the pool space is reserved for snapshots.

If you attempt to use a snapshot to restore your virtual disk, special care must be taken to make sure there is sufficient free space in the pool. The newly restored virtual disk is created from available free pool space. If there is insufficient space to create the new drive, the restore will fail. However, even if there is just enough space and other activity is occurring in the pool, the potential for a pool-full condition exists. In this case, Lifeguard may delete the snapshot that you are restoring from.

CAUTION: The consequence of utilizing Lifeguard is that during a restore Lifeguard can cause the loss of the original data represented in a snapshot. If the amount of free space goes below a specific threshold, Lifeguard deletes one or more snapshots to make more space available in the pool. See the “Snapshots and Restoring a Virtual Disk” section for more information.

The SWVR Lifeguard service is installed and automatically started. The service checks each drive letter on a system to see if it is a virtual disk or a snapshot. If it is a snapshot, Lifeguard checks the storage pool that the drive belongs to for its amount of current free space. This check is performed, by default, once every 10 seconds.

The TaskSmart N2400 appliance implementation of SWVR uses the following default settings for the SWVR Lifeguard service:

- Checks for pool-full situations once every 10 seconds
- Begins deleting snapshots when the free pool space drops below the 1,024-MB threshold

- Deletes the oldest snapshot first
- Continues to delete up to 12 snapshots at every 10-second interval until free pool space is above the threshold
- Reserves 30 percent of the total pool for snapshot use and restricts online volume growth from causing a pool-full condition by not allowing a volume to grow into this reserved space
- Deletes a snapshot, even if it is the only snapshot in existence

SWVR Lifeguard posts events in the Application Event Log and can be viewed using the Event Viewer. An event is entered for each drive that exceeds the threshold, and additional events will be entered when a snapshot is deleted.

NOTE: These default settings are different from those stated in the SWVR documentation included on the TaskSmart N2400 Documentation CD.

Modify Reserved Pool Space

Although it is not recommended, you can change the percentage of free pool space that is reserved for snapshots. If you are not using or planning to use snapshots, removing this reserved space should not cause a problem.

CAUTION: It is possible for data corruption to occur if the percentage of free pool space is removed and snapshots are used later without adding back the 30 percent reserved space. There is a default minimum of 1,056 MB of free space. It is not possible to set the reserved space less than this without activating Lifeguard service.

Increasing the percentage of free pool space poses no problem other than reserving a larger percentage of your pool.

To modify the percentage of free pool space:

1. Click **Command Prompt** on the TaskSmart N2400 console menu.

2. On the command line enter the command:

   mfsppp ***nn*** (where nn is the percentage of free pool space to reserve)

   For example:

   - ☐ **mfsppp 10** reserves 10 percent free pool space
   - ☐ **mfsppp 0** reserves 1,056 MB of free pool space (the minimum allowed)
   - ☐ **mfsppp 50** reserves 50 percent free pool space

3. Type **exit** to exit the command line window.

For help with the mfsppp command, type `mfsppp help` in the command line. Refer to the “Snapshots and Restoring a Virtual Disk” section earlier in this chapter.

IMPORTANT: Under no circumstances should Lifeguard functionality be changed.

Managing Space Usage with Quotas

Drive quotas enable administrators to control the allocation of drive space to individual users or groups of users. When quotas are enabled and properly configured, it is impossible for one person or group to consume all of the available space on a disk.

When quotas are enabled on a volume that already contains files, Windows calculates the drive space used by all users on the volume. The quota limit and warning level are then applied to all current users. Administrators can then modify quotas as needed. By enabling and then disabling quotas, administrators take advantage of the auditing capabilities provided by quotas, without reducing server performance.

To enable drive quotas:

1. Log on as Administrator on the TaskSmart N2400 appliance.
2. From the desktop, double-click **My Computer.**
3. In the My Computer interface, right-click on a virtual disk, and then select **Properties.**
4. In the Properties window, select the **Quota** tab.
5. Click the **Enable Quota Management** check box, and then click **OK.**

NOTE: If the volume is not formatted with the NTFS file system, or if you are not a member of the administrators group, the Quota tab is not displayed in the Properties dialog box of the volume.

NOTE: For more information about quotas, refer to online help for TaskSmart N2400 appliance quota help.

Chapter 3

Windows File System Administration

Common Internet File System User and Group Management

The Compaq TaskSmart N2400 appliance supports Network File System (NFS) and Common Internet File System (CIFS) protocols for file access over a network. The first protocol to be discussed is CIFS.

CIFS is the standard network file sharing mechanism used by Microsoft Windows NT clients and servers. It is a superset of the Server Message Blocks (SMB) network file sharing protocol.

Access to CIFS shares requires a network logon, providing username and password. A fundamental part of managing CIFS shares involves managing the users and groups that have access.

There are two administration environments for users and groups:

- **Workgroup—**All account information is stored locally.
- **Domain—**All account information is stored on a separate Windows NT or Active Directory Domain Controller.

NOTE: The appliance is not a domain controller for other servers. If user and group account information is locally stored, those accounts may be used only to authenticate logons to the appliance, resulting in a workgroup configuration.

Domain Compared to Workgroup

TaskSmart appliances can be deployed in a workgroup environment or in a domain environment. As previously mentioned, CIFS is a session-based, stateful network file sharing protocol. When mapping a network drive or a client machine, a user sends a logon credential to the server. This credential includes the username, password, and if appropriate, domain information. Using the credential, the server authenticates and provides the corresponding access to the user. When a TaskSmart appliance is deployed into a workgroup environment, all user and group account access permissions to file resources are stored locally on the appliance. .

By contrast, an appliance deployed into a domain environment uses the account database from the domain controller, with user and group accounts stored outside the appliance. The appliance integrates with the domain controller infrastructure

IMPORTANT: The TaskSmart N2400 appliance cannot act as a domain controller for other systems on the network.

Managing Users and Groups Effectively

Effective user and group management is dependent on how well users and groups are organized. Administrators typically create a small number of groups on the network, and then assign users to the appropriate group or groups. File system and share permissions can be applied at the group level, rather than at the user level. Because the number of groups is small, assigning the appropriate permissions to all users in a selected group, or groups, is more efficient.

Although each organization has specific conventions, following certain general guidelines makes administration simpler and more efficient. Because CIFS is dependent on users and groups to grant appropriate access levels to file shares, CIFS administration also benefits from a consistent user and group administration strategy.

Managing Usernames

It is recommended that usernames reflect a logical relationship between the username and the user who uses the account. It is important that rules are established to ensure that usernames are:

- Systematic
- Easy to follow and implement
- Similar (that is, the user’s account name corresponds with the user’s actual name)

Using a combination of the user’s first name, middle initial, and last name results in systematic usernames for every member of a particular organization. Common examples include:

- First initial followed by last name (jdoe for John Doe)
- First initial followed by middle initial and last name (jqpublic for John Q. Public)
- Last name followed by first initial (DoeJ for Jane Doe)

When two users have the same initials or name, several alternatives can be used to create unique names. For example, a number can be added to the end of the username (jdoe1 and jdoe2). You can also apply systematic naming rules (jdoe=John Doe and doej=Jane Doe).

Other conventions can be applied. Just ensure that conventions are both systematic and consistent.

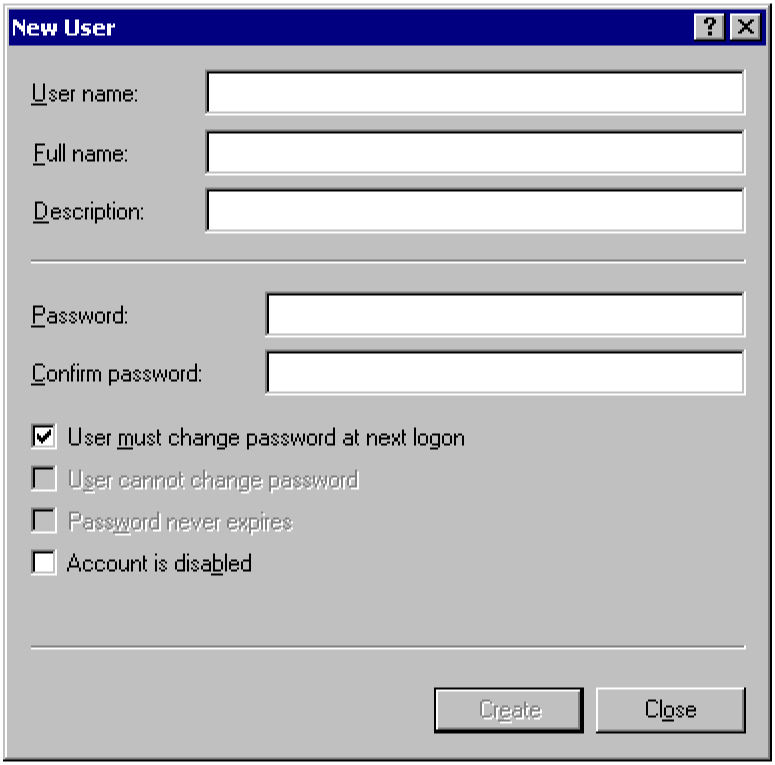
Workgroup Environment

To manage users and groups, click **Microsoft Management Console** on the TaskSmart N2400 console. Click **Core Operating System,** and then click **Local Users and Groups** to administer users and groups.

User Administration—Adding a User

To add a user:

1. Open the Users folder in **Local Users and Groups.**
2. Choose **Action,** then **New User.** A dialog box, shown in Figure 3-1, requests basic information about the user.
3. Enter the user name, full name, description, and password in the appropriate fields.



☑ User must change password at next logon
☐ User cannot change password
☐ Password never expires
☐ Account is disabled

Figure 3-1. New User dialog box

4. Four check boxes, described in Table 3-1, remain to be configured. Click to select the appropriate check box.

Table 3-1
New User Check Boxes

Check Box Name	Check Box Description
User must change password at next logon	Some CIFS clients have no way to change the password in a workgroup environment, and requiring a password change can cause problems. Deselect this option.
User cannot change password	Enabling this setting prevents the user from changing a password, even on Windows NT or Windows 2000 clients.
Password never expires	The particular user’s password never expires, and the user is not prompted to change the password. Again, because Windows 95 and Windows 98 have no client-side provision for changing passwords, select this box to avoid problems.
Account is disabled	If selected, the account cannot be used.

User Administration—Changing a Client Password

Follow these steps to change a Windows NT or Windows 2000 client password from the client machine, not the appliance.

1. Press **Ctrl+Alt+Delete**.
2. Choose **Change Password.**
3. Select the domain name in the Log On To box to allow the password to be changed.

IMPORTANT: The Change Password option is not available for Windows 95 or Windows 98 clients.

User Administration—Deleting a User

Follow these steps to delete a user:

1. Open the user's folder in Local Users and Groups.
2. Select the desired user name.
3. Select **Action,** and then **Delete.** A dialog box is displayed to confirm the deletion.
4. Choose **Yes** to delete.

User Administration—Modifying a User

Existing user names can be modified. Follow these steps to modify a user name:

1. Open the user's folder in Local Users and Groups.
2. Select the desired user.
3. Choose **Action,** and then **Rename.**
4. Type the desired user name.

User Administration—Modifying a User's Password

Follow these steps to modify a user's password:

1. Open the user's folder in Local Users and Groups.
2. Select the username, click **Action,** and then click **Set Password**. Figure 3-2 illustrates the Set Password dialog box.

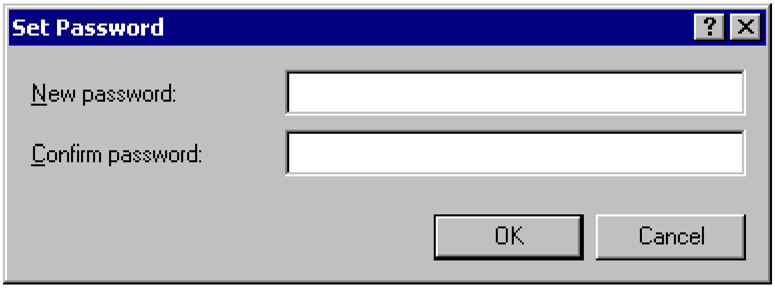
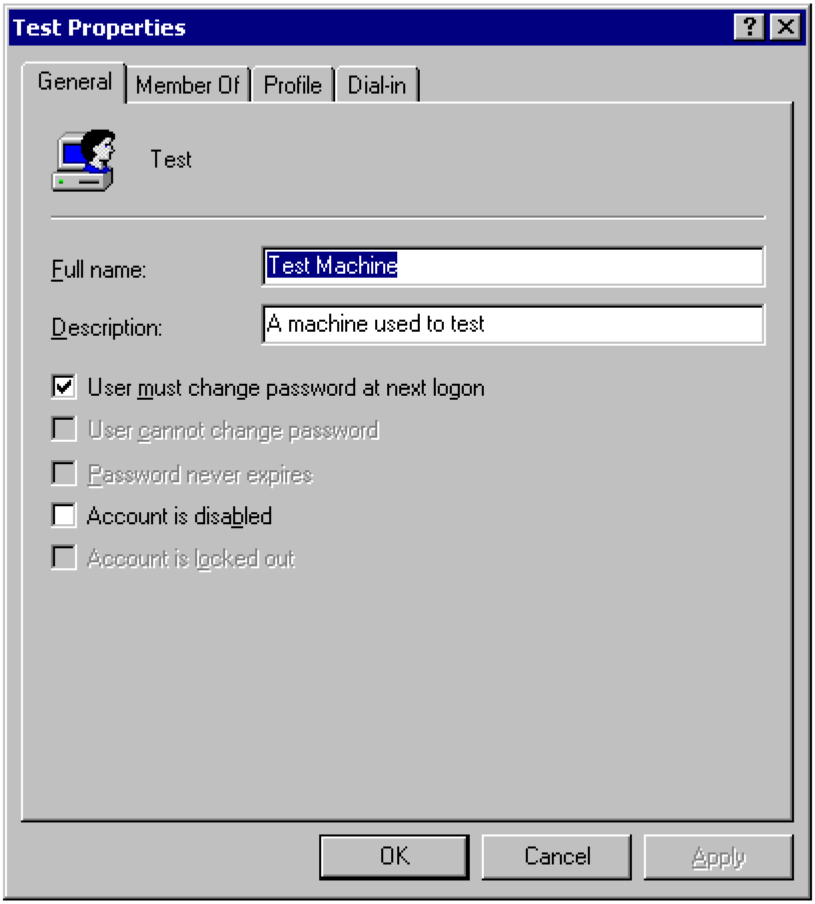


Figure 3-2. Set Password dialog box

3. Type the new password, and then type it again to confirm it.
4. Click **OK.**

User Administration—Modifying Other User Properties

To modify other user properties, double-click the user name to launch the User Properties dialog box. See Figure 3-3.



Full name: Test Machine

Description: A machine used to test

☑ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

☐ Account is locked out

Figure 3-3. Modify User Properties dialog box, General tab

The Full name and Description fields can be modified within the General tab, along with the following properties:

> **NOTE:** The first four properties in the following list are identical to the properties described in the “User Administration—Adding a User” section earlier in this chapter.

- User must change password at next logon
- User cannot change password
- Password never expires
- Account is disabled
- Account is locked out

This option, when checked, locks out the user and prevents any access by that user to network file shares. This property can be automatically enabled if a particular user repeatedly fails to properly enter a password when trying to map a network share. If this occurs, deselecting the checkbox restores user access.

Three additional tabs are available to modify user properties.

- **Member Of—**Allows the particular user placement into one or more groups.
- **Profile—**In a Workgroup environment, profiles apply only when a user logs directly onto the appliance console.
- **Dial-in—**For direct dial-in to the appliance console. This model is not typical.

By default, the user is a member of the Users group only when configured in a workgroup environment. The **Member Of** tab is illustrated in Figure 3-4. To remove a user from a particular group, select the user, and then click **Remove.**

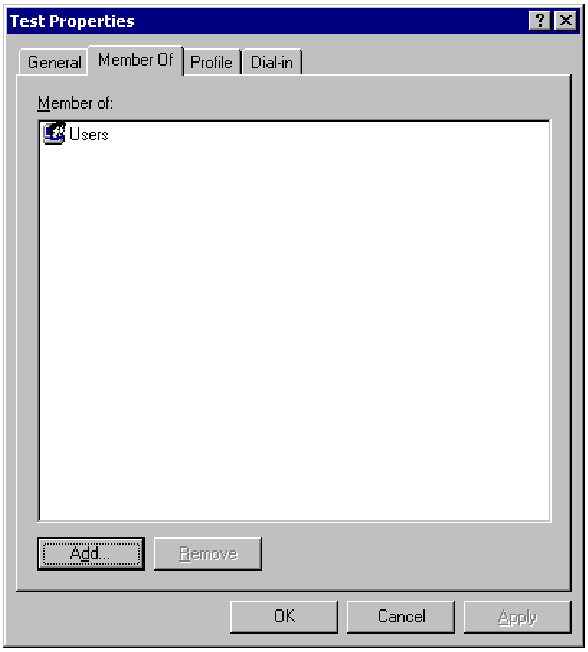
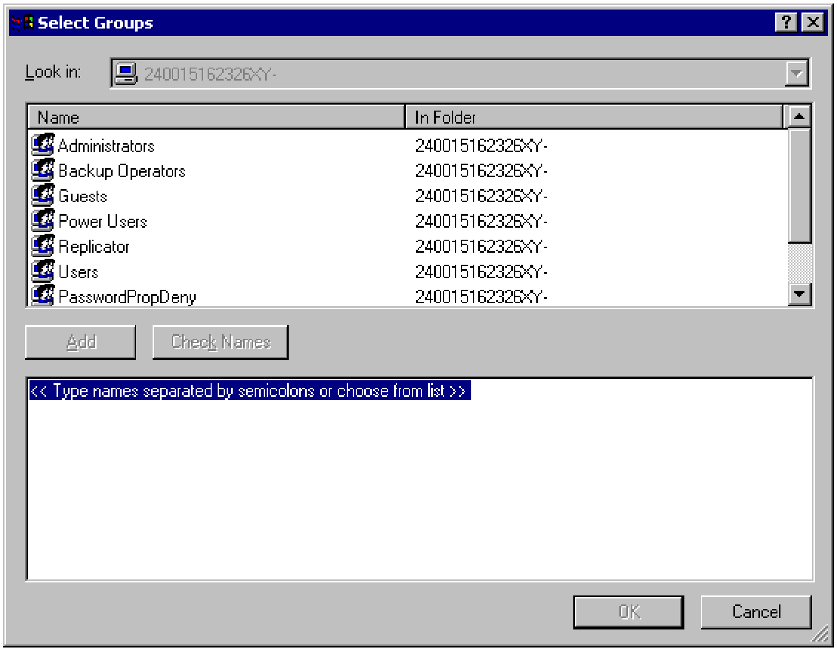


Figure 3-4. User Properties dialog box, Member Of tab

To add the user to other groups, choose **Add** on the Select Groups dialog box. See Figure 3-5. Then, select the groups that apply and click **OK.**



Name	In Folder
Administrators	240015162326XY-
Backup Operators	240015162326XY-
Guests	240015162326XY-
Power Users	240015162326XY-
Replicator	240015162326XY-
Users	240015162326XY-
PasswordPropDeny	240015162326XY-

<< Type names separated by semicolons or choose from list >>

Figure 3-5. Select Groups dialog box

Group Administration—Adding a Group

To add a group, follow these steps:

1. Open the Groups folder in the Local Users and Groups section.
2. Select **Action,** and then **New Group.** The dialog box in Figure 3-6 is displayed.

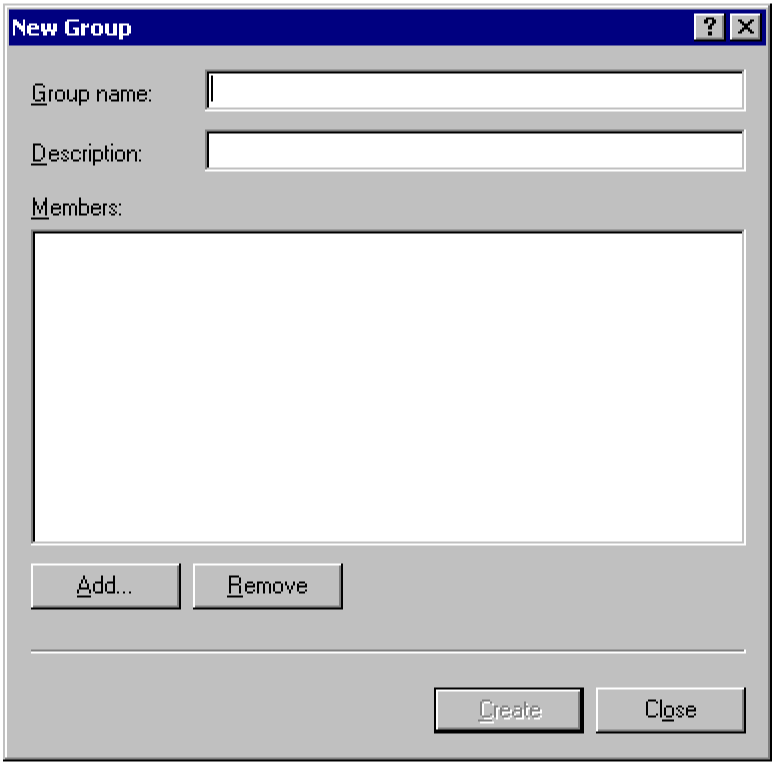


Figure 3-6. New Group dialog box

3. Enter the desired group name.
4. Enter a description.

5. To add users or groups to the newly created group, click **Add.** The Select Users or Groups dialog box shown in Figure 3-7 is displayed.

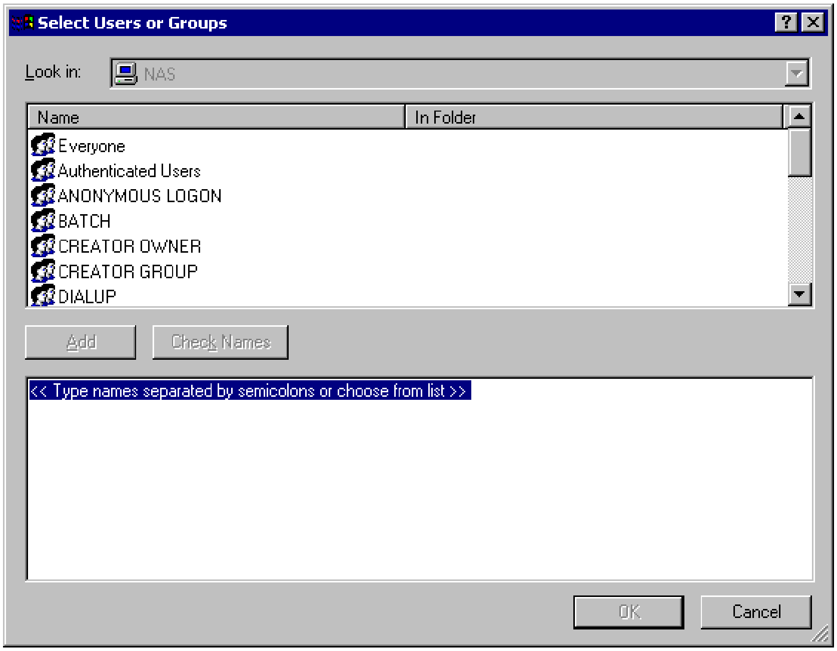


Figure 3-7. Select Users or Groups dialog box

The Select Users or Groups dialog box contains the Look in drop-down list. Users and groups from external domains can be added to a local group that has certain access rights to the workgroup server, creating a trust relationship between a workgroup server and a Windows domain. Client members of the particular domain then have access to the appropriate shares on the TaskSmart N2400 appliance that is configured in a workgroup environment. Click the **OK** button to save changes.

NOTE: After users or other groups are added, they can be removed by clicking Remove when the user or group is highlighted.

Group Administration—Deleting a Group

A group can be deleted, using the MMC.

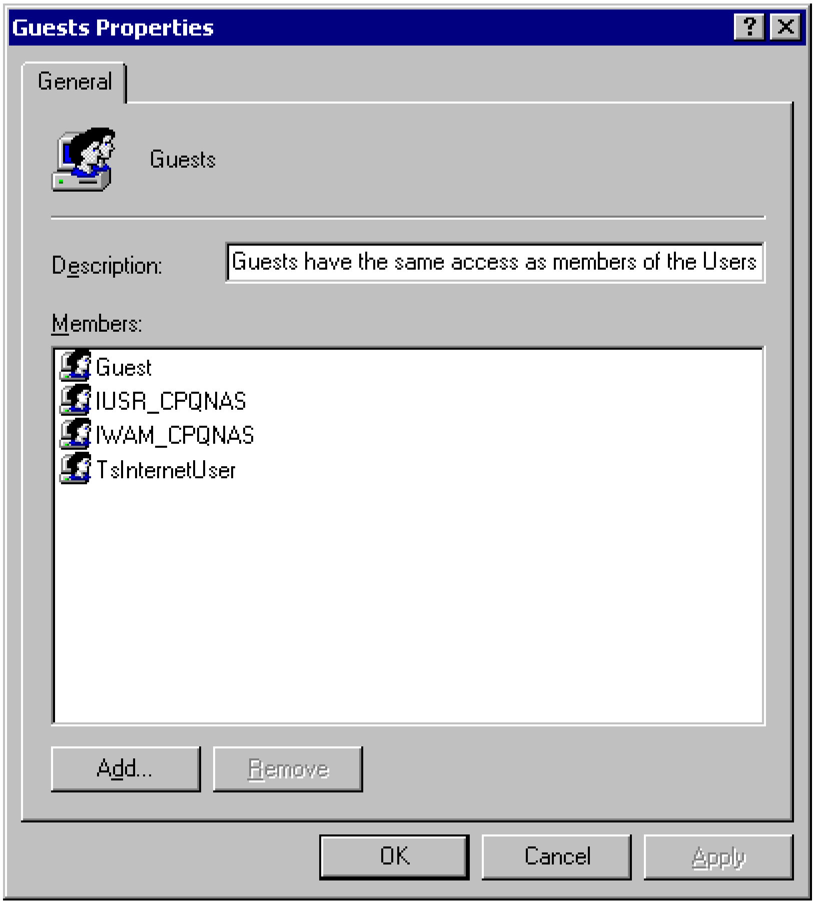
1. Open the Groups folder **Local Users & Groups** section.
2. Select the desired group.
3. Click **Action,** and then **Delete.**

Group Administration—Modifying a Group

Existing group names and group properties can be modified. Follow these steps to modify a group name:

1. Open the Groups folder **Local Users & Groups** section.
2. Select the desired group.
3. Click **Action,** and then **Rename.**
4. Enter the desired group name.

To modify other properties, double-click the desired group name. The Guest Properties dialog box, illustrated in Figure 3-8, is displayed.



Description: Guests have the same access as members of the Users

Members:
- Guest
- IUSR_CPQNAS
- IWAM_CPQNAS
- TsInternetUser

Figure 3-8. Guests Properties dialog box

From the Guest Properties screen, guest users can be added to, or removed from, the group by following the same procedure as for client users. The dialog box that is displayed is identical to the Select Groups dialog box illustrated in Figure 3-5.

Domain Environment

Administering users and groups in a domain environment is similar in a mechanical sense to administering them in a workgroup environment. If using an Active Directory domain controller, the Computer Management tool allows for adding, modifying, and removing users in the same MMC context as in a workgroup environment. The concepts, however, are very different.

When in a domain environment, the server is a member of the domain. The domain controller is a repository of accounts and account access for the appliance. Client machines are also members of the domain, and users log on to the domain through their Windows clients. The domain controller also administers user accounts and appropriate access levels to resources that are a part of the domain. Additional information about planning for domain environments can be found at the Compaq *ActiveAnswers*™ website in the eBusiness Infrastructure solutions area:

http://www.compaq.com/ActiveAnswers/

The configurations of the domain controller or controllers are reflected on the TaskSmart N2400 appliance, because it obtains user account information from the domain controller or controllers when deployed in a domain environment. The appliance cannot act as a domain controller itself.

IMPORTANT: The domain administration tasks described, whether for an Active Directory domain or a Windows NT 4.0 domain, are tasks that configure the domain controller or controllers, and not the TaskSmart N2400 appliance.

Active Directory Domain—Administering Users and Groups

The process of adding, removing, or modifying users and groups in an Active Directory domain environment is similar to that for administering users and groups in a workgroup environment. There are three essential differences:

- Users and groups are administered on the Active Directory domain controller rather than on the appliance.
- Computer accounts must be administered in the domain as well as user and group accounts.
- A different tool is used to manage domain accounts.

You administer user, group, and computer accounts in an Active Directory domain environment using one of two methods:

- From the Active Directory domain controller console, not the TaskSmart N2400 appliance

  On the taskbar, select **Start, Programs, Administrative Tools,** and then **Active Directory Users and Computers.** This selection launches an MMC that allows for the administration of user, group, and computer accounts in the domain.

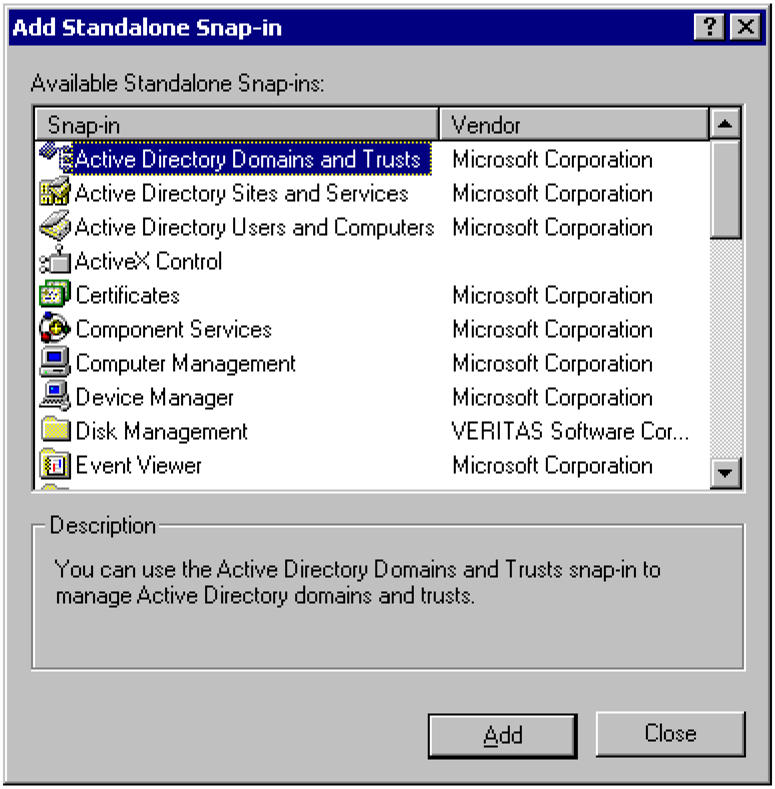
- Remotely from a client machine that points to the Active Directory domain controller

1. Log on using a Windows 2000 client as a domain administrator.

IMPORTANT: The administrator must have sufficient access rights to administer users and groups on the domain.

---

2. Choose **Start,** and then **Run.**
3. Type `MMC.EXE` in the dialog box.
4. Select **Console,** and then **Add/Remove Snap-in.**
5. Click **Add.** The Add Standalone Snap-in dialog box is displayed, as shown in Figure 3-9.



Snap-in	Vendor
Active Directory Domains and Trusts	Microsoft Corporation
Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Computers	Microsoft Corporation
ActiveX Control	
Certificates	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation
Disk Management	VERITAS Software Cor...
Event Viewer	Microsoft Corporation

Description

You can use the Active Directory Domains and Trusts snap-in to manage Active Directory domains and trusts.

Figure 3-9. Add Standalone Snap-in dialog box

6. With the Active Directory Users and Computers snap-in selection highlighted, click **Add.**

7. After the snap-in is added, you must connect to the appropriate domain to enable remote administration. To do this:
   a. Select the Active Directory Users and Computers snap-in.
   b. Click **Action,** and then **Connect to Domain.**
   c. A dialog box asks you to enter the domain name of the Active Directory to be administered.
   d. Enter the domain name.

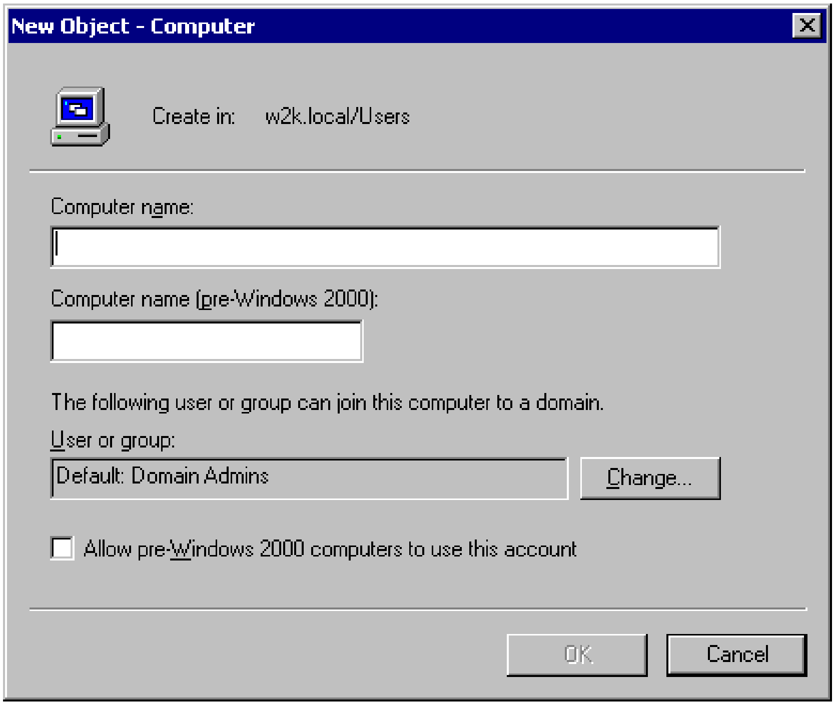
NOTE: Full name resolution must be properly configured in the network environment in which the domain resides. Be sure that DNS, hosts/LMHOSTS files, or both are properly set up.

NOTE: Users with sufficient permission to administer the domain must be logged on to the client machine. Typically, such users are members of the domain administrators group, but other groups can also have administrative permissions.

Active Directory Domain—Adding the TaskSmart N2400 Appliance

After you have properly made the connections to your domain through the Active Directory Users and Computers snap-in, you can begin administering this portion of the Active Directory. The first task is to add the TaskSmart N2400 appliance to the Active Directory by following these steps:

1. Select the **Computers** folder in the snap-in.
2. Choose **Action, New, Computer.** This process launches the New Object - Computer dialog box, pictured in Figure 3-10.



New Object - Computer

Create in: w2k.local/Users

Computer name:

Computer name (pre-Windows 2000):

The following user or group can join this computer to a domain.

User or group:
Default: Domain Admins

☐ Allow pre-Windows 2000 computers to use this account

Figure 3-10. New Object - Computer dialog box

3. Enter the appropriate computer name in the first field.

   NOTE: The Computer name (pre-Windows 2000) field automatically populates. The Allow pre-Windows 2000 computers to use this account check box option is not relevant and must remain unchecked, because the appliances are based on Windows 2000.

4. If necessary, click **Change** to change the default group for the computer account; however, remember that the computer account (not the user accounts) accesses the Active Directory through the computer.
5. Select **OK.**

Active Directory Domain—Creating User and Group Accounts

To create user and group accounts on the Active Directory console, you can use the same Active Directory Users and Computers snap-in used in the "Active Directory Domain—Adding the TaskSmart N2400 Appliance" section earlier in this chapter. Instead of using the Computers folder of the snap-in, however, use the Builtin folder and the Users folder.

For help, select the appropriate MMC snap-in, and then click **Help** from the Console menu. Documentation for planning and deploying the Active Directory can be obtained at the Compaq ActiveAnswers website in the eBusiness Infrastructure solutions area:

http://www.compaq.com/ActiveAnswers/

Active Directory—Builtin Folder

The Builtin folder contains information about all the groups added to a default Active Directory. Default Active Directory folders contain the following groups:

- Account Operators
- Administrators
- Backup Operators
- Guests
- Pre-Windows 2000 Compatible Access
- Print Operators
- Replicator
- Server Operators
- Users

NOTE: References to users and groups are presented in the context of the Users group, except when demonstrating how to create a new group.

More information about the use of groups is available in the eBusiness Infrastructure solutions area, in Microsoft Active Directory operating system documentation, or at the following websites:

http://www.compaq.com/ActiveAnswers

http://www.microsoft.com

Active Directory—Creating a New User

The Users folder is the repository for displaying all the users and groups on the Active Directory and is useful when modifying the properties of a particular user or group. One of the basic functions of the Users folder is the ability to add users and groups.

1. Highlight the Users folder in the Active Directory Users and Computers snap-in.
2. Select **Action, New, User.** The New Object - User dialog box shown in Figure 3-11 is displayed.

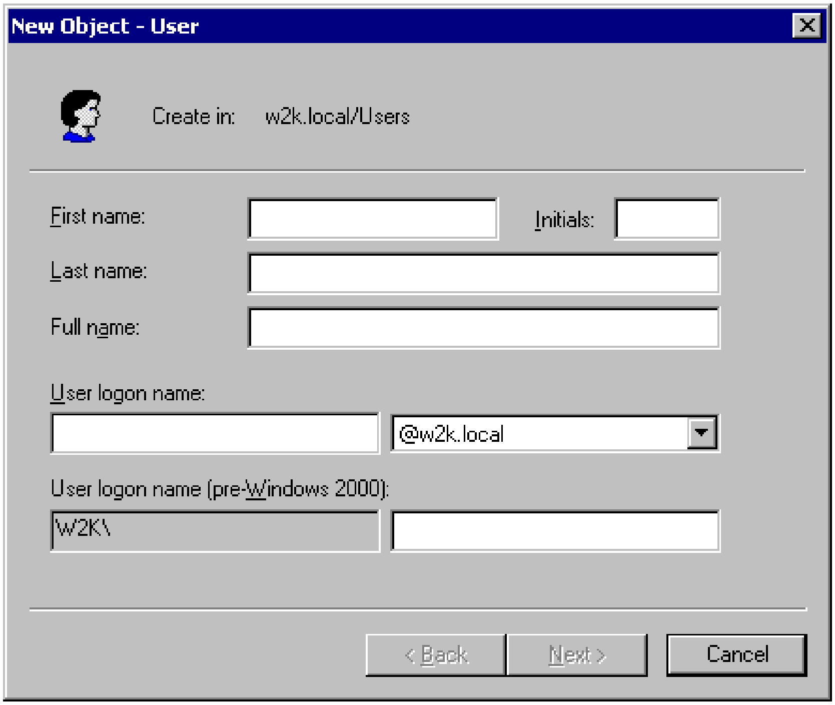


Figure 3-11. New Object - User dialog box, user information

3. Enter the information into the text boxes.

   NOTE: The logon context is USER@DOMAIN in the Active Directory, but the legacy logon context of DOMAIN\USER is supported.

   After entering data in the First name, Initials, and Last name fields, the Full name value automatically generates. When entering the User logon name, the pre-Windows 2000 User logon name fills in automatically. It is advisable to accept the default entry, particularly if there are older machines included on the network infrastructure.

   NOTE: If multiple domain controllers are used, Active Directory or otherwise, it is recommended that user account names be unique across domains. Unique naming makes NFS administration easier.

4. When the required information is entered, initial user values have been set. Click **Next** and the dialog box depicted in Figure 3-12 is displayed.

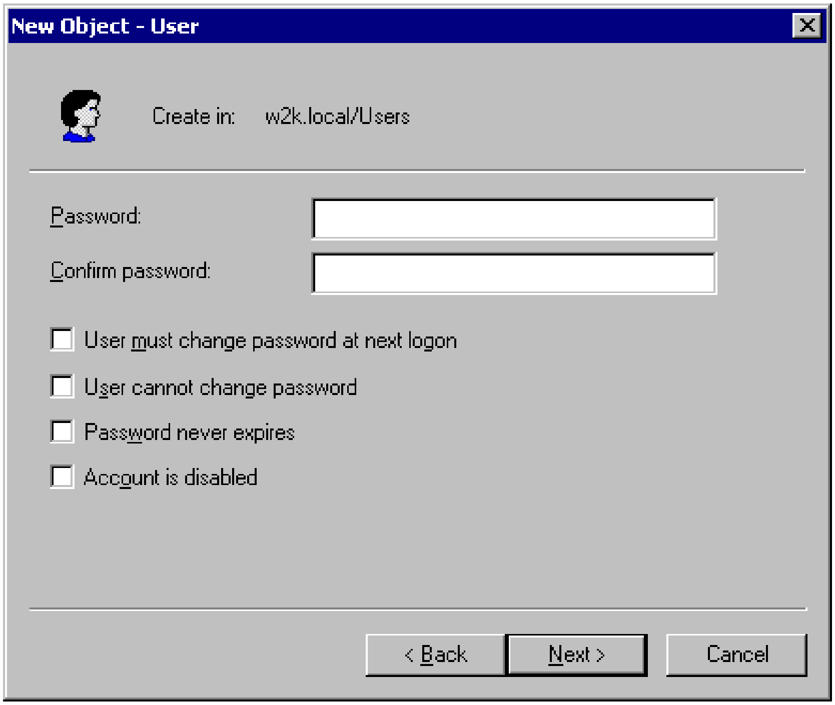


Figure 3-12. New Object - User dialog box, password information

5. Enter the password information.

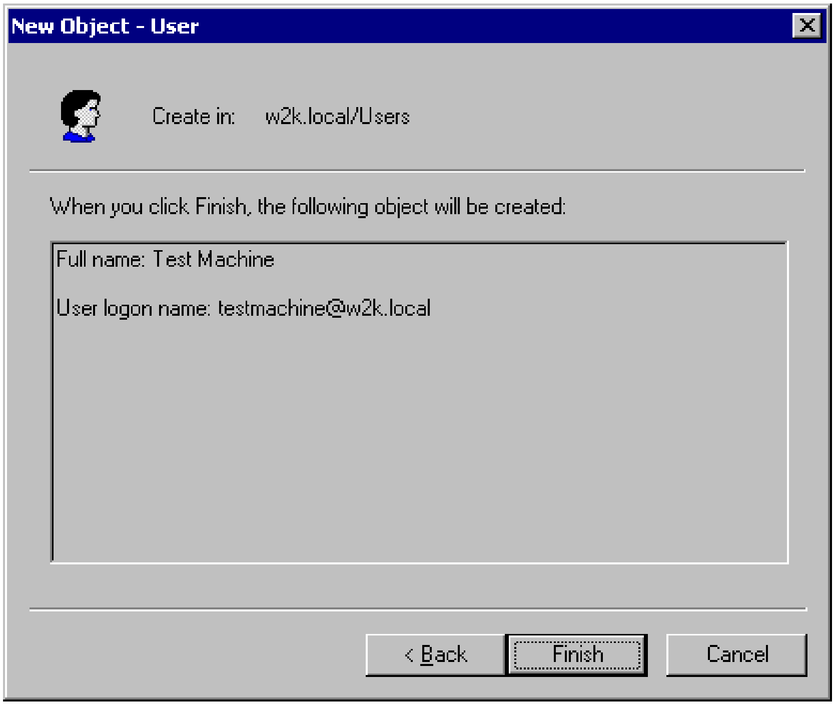
6. Click the appropriate check boxes. The check boxes are identical to the ones that are displayed when you create a new user in a workgroup environment, except that these user properties are stored in the Active Directory rather than locally on the appliance.

NOTE: In this environment, it is acceptable to force the user to change a password at the next logon. Users who need to access CIFS file resources on an appliance deployed in an Active Directory environment log on to the Active Directory from their remote workstations. The Active Directory appropriately forces remote users to change passwords to ensure security.

Table 3-2
Active Directory User Account Characteristics

Characteristic	Summary
User must change password at next logon	Checking this box requires the user to change the password at next logon to the domain.
User cannot change password	If checked, the user cannot modify the password.
Password never expires	If enabled, the domain controller never requires a user to change a password. However, the user can voluntarily change the password.
Account is disabled	If this box is checked, the account is disabled and the user can no longer log on to the domain. However, the account remains on file. If a user forgets a password, failed logon attempts can automatically disable the account. The account can be re-enabled here.

7. Click **Next** when all user information is entered. The dialog box in Figure 3-13 is displayed.



When you click Finish, the following object will be created:

Full name: Test Machine

User logon name: testmachine@w2k.local

Figure 3-13. New Object - User dialog box, information summary

8. Verify the New Object - User summary information.

9. Click **Finish** to create the new user. If edits are needed, click **Back** and make the appropriate changes.

Active Directory—Deleting a User

A user can be deleted from the Active Directory by following these steps:

1. Open the Active Directory Users folder.
2. Highlight the user name that you want to delete.
3. Select **Action,** and then **Delete.**
4. Click **Yes** to confirm the deletion.

Active Directory—Modifying a User

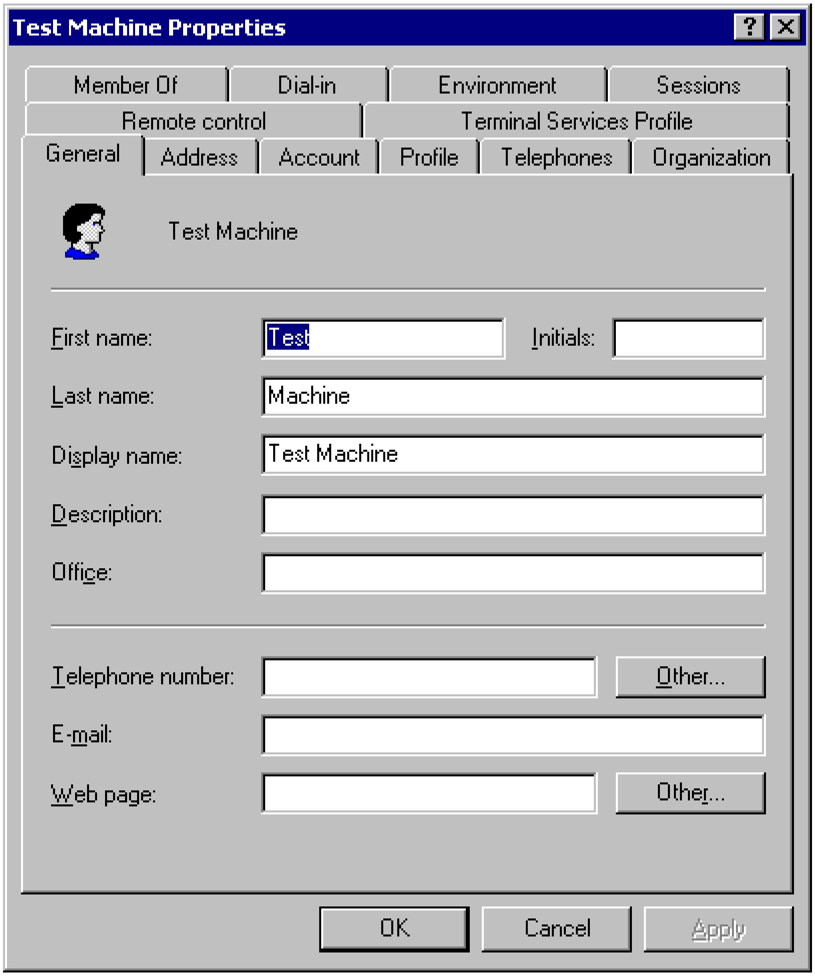
Users can also be modified in the Active Directory using the following steps:

To rename a user associated with a specific username:

1. Open the Active Directory Users folder.
2. Highlight the user that you want to modify.
3. Select **Action,** and then **Rename.**
4. Enter the new name for the user.

NOTE: This procedure changes only the information in the Full name field, not the name of the account associated with the user.

To make other modifications, double-click the desired user in the list. A dialog box similar to Figure 3-14 is displayed.



Test Machine

First name: Test

Last name: Machine

Display name: Test Machine

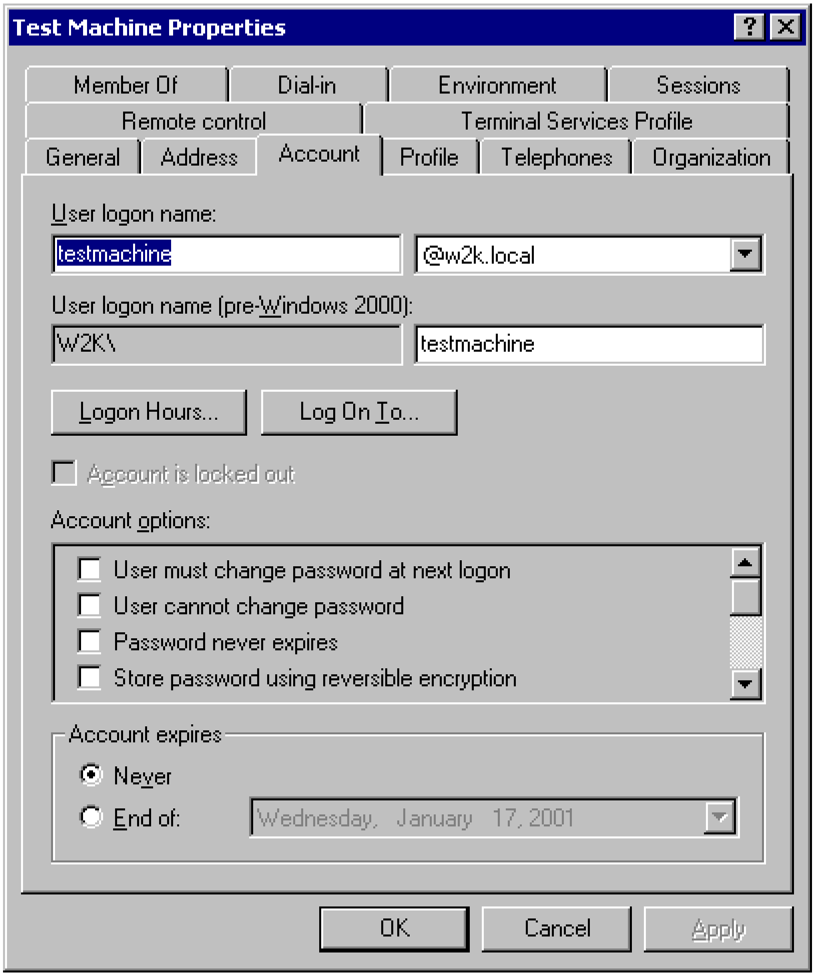
Figure 3-14. Modify User Properties - General tab dialog box

The information entered on the General tab is useful contact documentation for the user and is for informational purposes only. Other Properties apply to how users interact with the appliance. These are:

- Account
- Profile
- Member Of
- Sessions

Modifying a User—Account Properties Tab

The Account tab allows for modifications associated with the user logon account. The dialog box pictured in Figure 3-15 reflects an example of account information about user testmachine.



User logon name:
testmachine @w2k.local

User logon name (pre-Windows 2000):
W2K\ testmachine

☐ Account is locked out

Account options:
☐ User must change password at next logon
☐ User cannot change password
☐ Password never expires
☐ Store password using reversible encryption

Account expires
● Never
○ End of: Wednesday, January 17, 2001

Figure 3-15. Modify User Properties - Account tab dialog box

NOTE: The Windows 2000 and pre-Windows 2000 logon names are identical to the same fields used in the New User Wizard.

In an Active Directory environment, the administrator can establish the user's logon hours and the client machines accessed. Although these parameters affect the way file-sharing clients interact with the appliance, they are better documented elsewhere. The information in Table 3-3 describes most of the policies for managing user accounts.

Table 3-3
Managing User Account Properties

Policy	Description
User must change password at next logon	Checking this box requires the user to change password at the next logon to the Active Directory.
User cannot change password	If checked, the user cannot modify password.
Password never expires	If enabled, the Active Directory never requires a user to change a password. This check box does not prevent the user from doing so voluntarily.
Store password using reversible encryption	Passwords are normally stored in the Active Directory using one-way encryption. Checking this box causes the user's password to be stored using a two-way encryption algorithm. As such, it is less secure.
Account is disabled	If this box is checked, the account is disabled, and the user can no longer log in to the Active Directory; however, the account remains on file. Failed logon attempts can automatically disable the account. The account can be re-enabled here.
Smart card required for interactive logon	For clients that store user authentication information on Smart cards, enabling this check box requires authentication by Smart card rather than by username and password.

continued

Table 3-3
Managing User Account Properties *continued*

Policy	Description
Account is trusted for delegation	Refer to the Active Directory resource for complete information.
Account is sensitive and cannot be delegated	Refer to the Active Directory resource for complete information.
Use DES encryption types for this account	Refer to the Active Directory resource for complete information.
Do not require Kerberos preauthentication	Refer to the Active Directory resource for complete information.

Modifying a User—Profile Properties Tab

The Profile tab sets the properties that designate which areas of network environment the user receives at logon. The profile can enable a logon script that maps network drives on the client to CIFS shares presented by the appliance. A user’s home folder can also be configured to automatically map to a CIFS share on the appliance. More information is available in your Active Directory documentation. The Profile dialog box is illustrated in Figure 3-16.

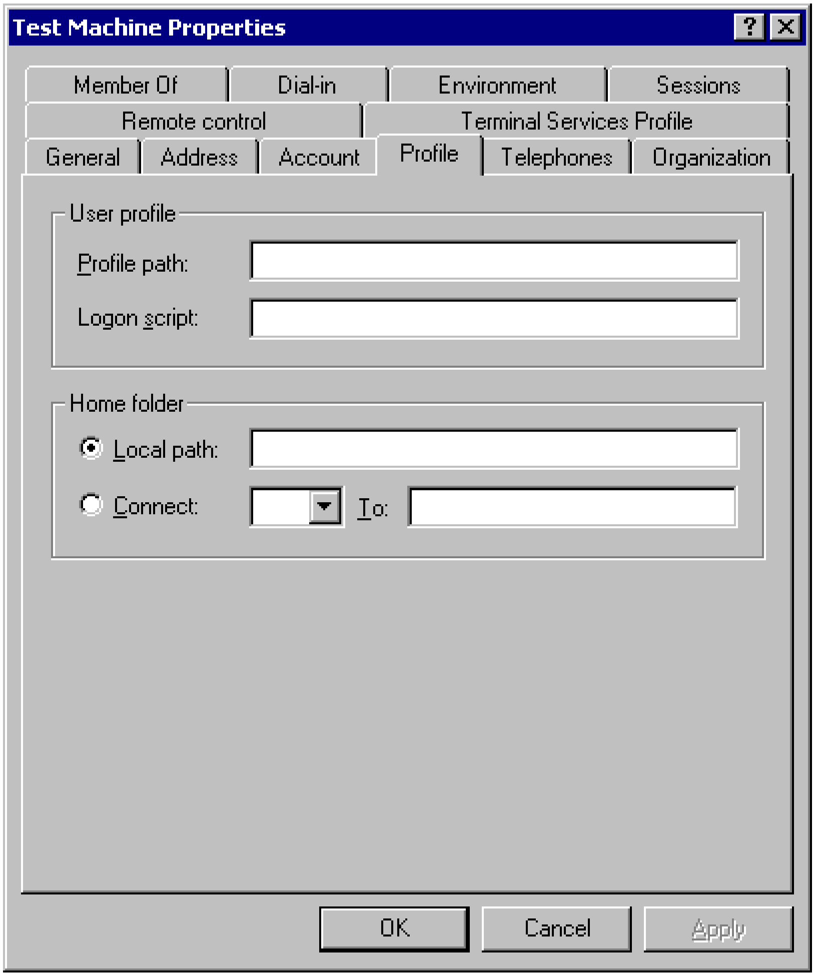
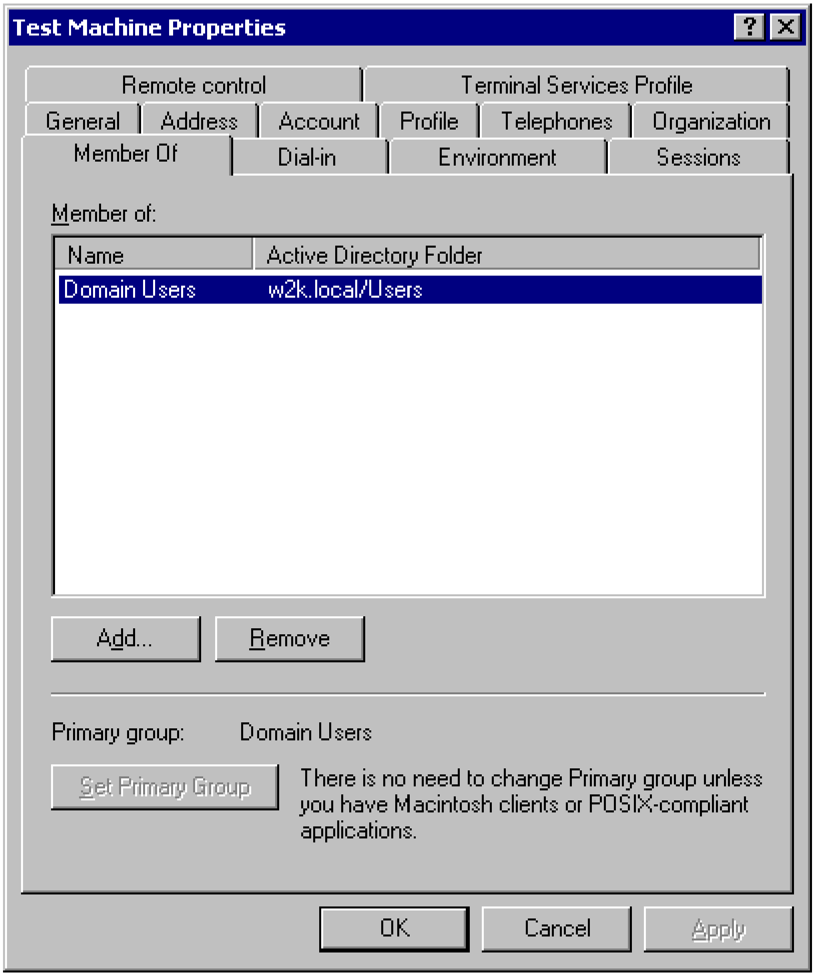


Figure 3-16. Modify User Properties - Profile tab dialog box

Modifying a User—Member Of Tab

The Member Of tab lists the groups that apply to a particular user. The member information is important because CIFS is a stated protocol that uses user and group authentication to provide or restrict access to file resources.

Placing a user strategically into one or more groups means that the administrator can provide or restrict access by group rather than by user. Because there are usually more users than groups, effective placement of users into groups is critical to efficient share management.



Member of:

Name	Active Directory Folder
Domain Users	w2k.local/Users

Primary group: Domain Users

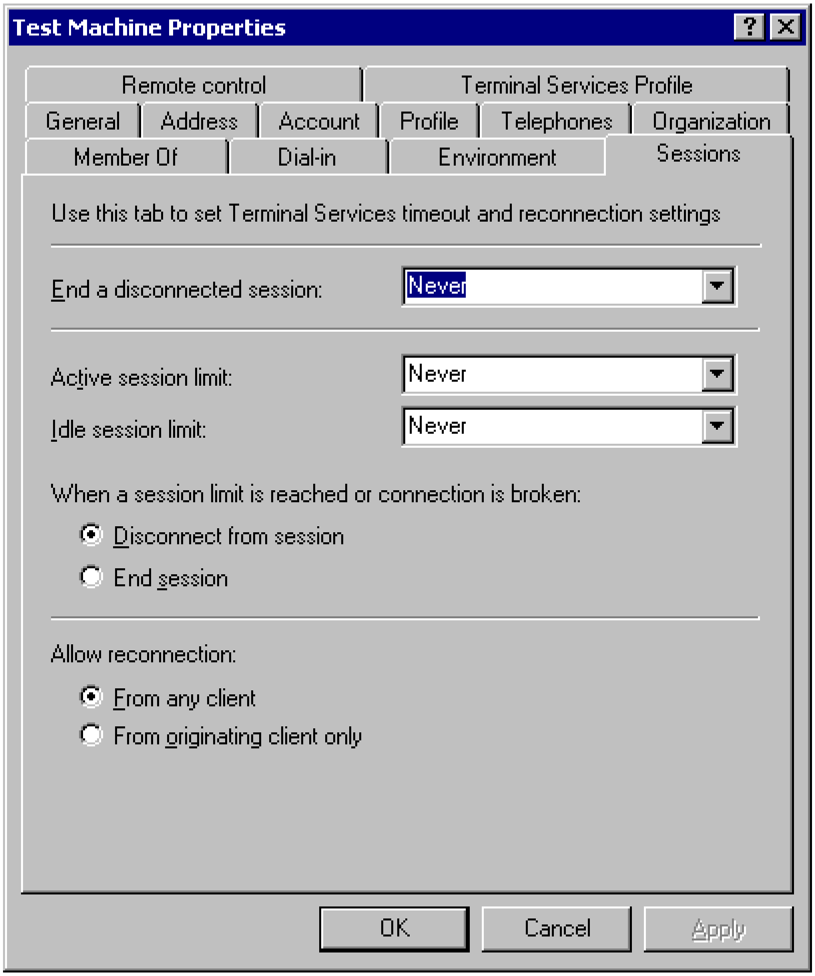
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Figure 3-17. Modify User Properties - Member Of tab dialog box

The Primary Group section of the dialog box refers to the first group that the user is associated with when applications request user information. Some POSIX-compliant applications differentiate between the primary group and other member groups when deciding on group contexts within which to run an application. It is usually unnecessary to change primary group member information in a CIFS file-serving environment. It can be useful, however, to change member information when using the Active Directory to control access to servers other than a TaskSmart N2400 appliance server.

Modifying a User—Sessions Tab

The Sessions tab allows the administrator to set properties that instruct the Active Directory how to manage client sessions that are disconnected or timed out. Because the CIFS protocol is session based, the manner in which disconnected sessions are handled can affect the way clients interact with a TaskSmart N2400 appliance. The dialog box in Figure 3-18 illustrates how sessions information is entered.



Use this tab to set Terminal Services timeout and reconnection settings

End a disconnected session: Never

Active session limit: Never

Idle session limit: Never

When a session limit is reached or connection is broken:

● Disconnect from session

○ End session

Allow reconnection:

● From any client

○ From originating client only

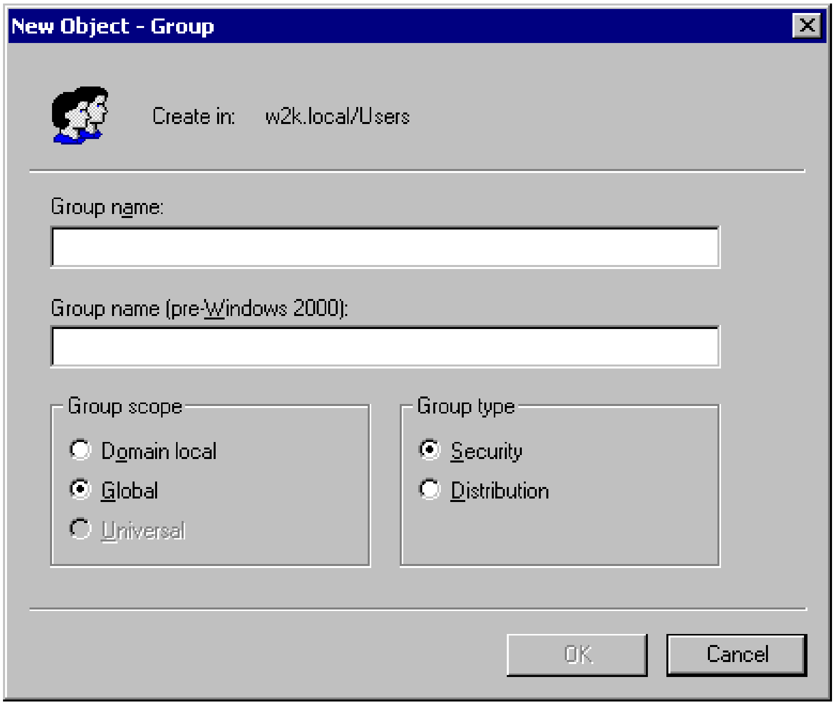
Figure 3-18. Modify User Properties - Sessions tab dialog box

By default, disconnected sessions are not ended, even if the client-server connection is accidentally broken, as in the case of a faulty network cable. The default also allows any client on the network to reconnect to a disconnected session. Potential security ramifications can affect file-serving functions and the integrity of the data on an appliance. For detailed security information, refer to the Microsoft Active Directory Documentation included with Windows NT.

Active Directory—Creating a New Group

Follow these instructions to create a new group in the Active Directory:

1. Highlight the Users folder in the Active Directory Users and Computers snap-in.
2. Select **Action, New, Group.** The New Object - Group dialog box, shown in Figure 3-19, is displayed.



New Object - Group

Create in: w2k.local/Users

Group name:

Group name (pre-Windows 2000):

Group scope

○ Domain local

● Global

○ Universal

Group type

● Security

○ Distribution

Figure 3-19. New Object - Group dialog box

For information on how to set up and deploy the Active Directory under Windows 2000, or about the best practices for administering an Active Directory domain, see the eBusiness Infrastructure solutions website:

http://www.compaq.com/ActiveAnswers

Additional information can also be obtained by selecting the appropriate MMC snap-in, and then choosing **Help** from the Console menu.

Windows NT Server 4.0 Domain

Integrating an appliance into a Windows NT 4.0 domain is similar to adding it to an Active Directory domain. The only difference is on the domain itself. The tasks to be performed on the appliance are identical:

1. The computer account is created in the domain.
2. The appliance, as a domain client, registers itself with the domain to enable the account.
3. The appliance is restarted and can be used within the domain context.

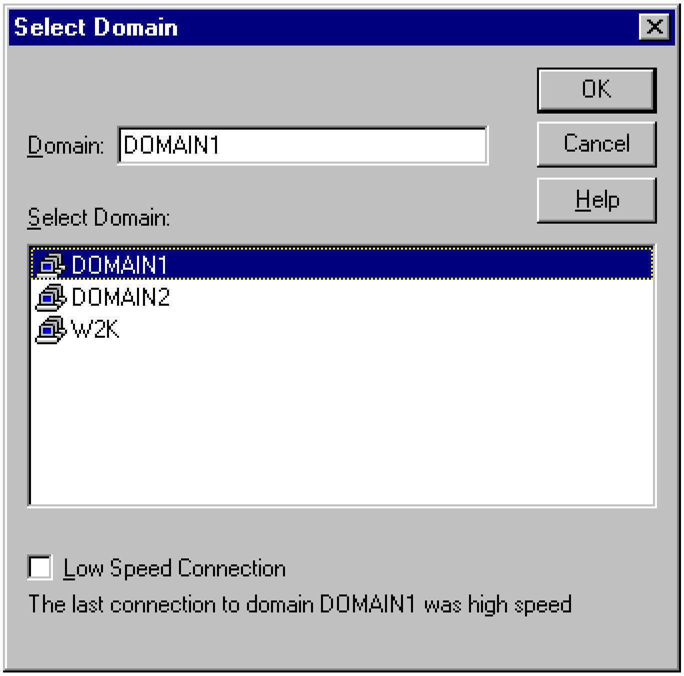
Windows NT Server 4.0 Domain—Server Manager

Server Manager is the administrative tool within Windows NT 4.0 for adding computers to a domain. Server Manager is accessible from any Windows NT 4.0 server on the same network as the domain controller or controllers. For additional help with integrating an appliance into a Windows NT 4.0 domain, select **Help** from the main Server Manager menu.

To launch Server Manager from the Windows NT taskbar, click **Start**, **Programs**, **Administrative Tools**, **Server Manager**. The Server Manager application displays a default window that includes a list of all server and workstation accounts in the domain.

If the server is not directly running on a domain controller, it must be connected to the domain. The following instructions describe how to connect to the domain:

1. Select **Computer** from the Server Manager menu.
2. Select **Domain** from the Server Manager menu.



Domain: DOMAIN1

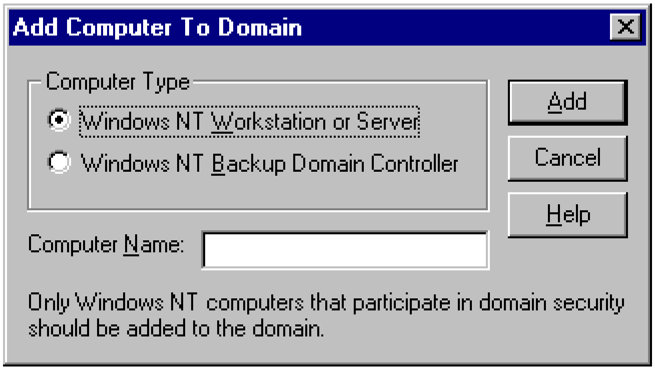
☐ Low Speed Connection

The last connection to domain DOMAIN1 was high speed

Figure 3-20. Select Domain dialog box, Server Manager

3. Select the appropriate domain from the list box, or type the domain directly into the Domain field.

To create a computer account in the domain for the appliance, select **Computer,** and then **Add to Domain** from the Server Manager menu. A dialog box similar to Figure 3-21 is displayed.



● Windows NT Workstation or Server
○ Windows NT Backup Domain Controller

Computer Name:

Only Windows NT computers that participate in domain security should be added to the domain.

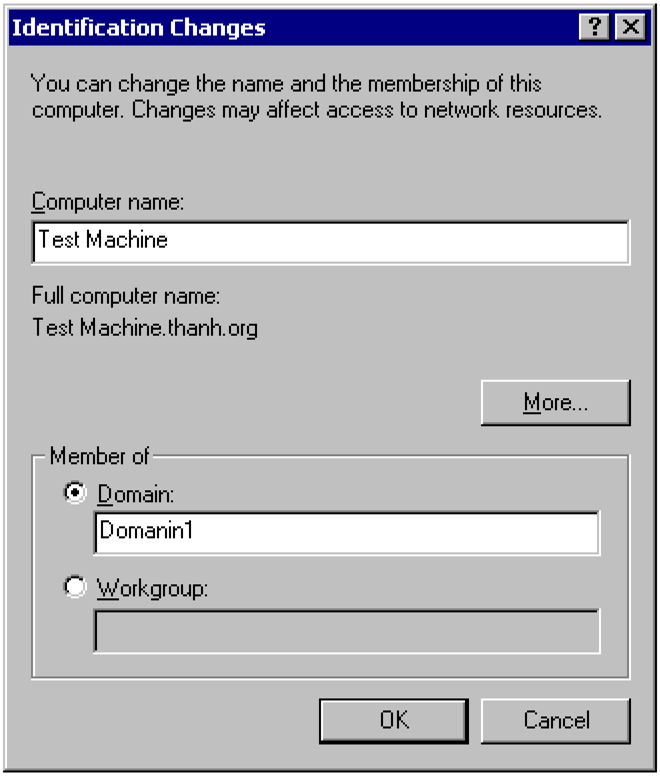
Figure 3-21. Add Computer to Domain dialog box

Select the Windows NT Workstation or Server option button, enter the appropriate computer name, and then click **Add.**

When this process is complete, you can return to the TaskSmart N2400 console to register the appliance with the domain.

Setting the Computer Identity

After the computer account for the appliance has been created in the domain, access the TaskSmart N2400 console. Right-click the My Computer icon on the appliance desktop, and then choose **Properties.** Then, select the Network Identification tab. Click the **Properties** button. A dialog box similar to Figure 3-22 is displayed.



Identification Changes

You can change the name and the membership of this computer. Changes may affect access to network resources.

Computer name: Test Machine

Full computer name:
Test Machine.thanh.org

Member of
● Domain: Domanin1
○ Workgroup:

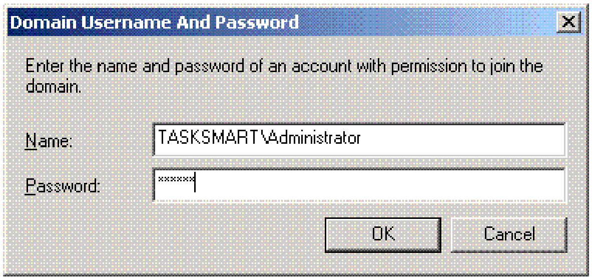
Figure 3-22. Identification Changes dialog box

Follow these instructions to place the appliance into the domain:

1. Select the **Domain** option button under Member Of.
2. Enter the name of the domain.

NOTE: The domain name is likely different from the server name of the domain controller. Be sure to enter the domain name.

3. Click **OK.** The Domain Username and Password screen is displayed and asks for the name of a user with permission to join the domain. See Figure 3-23.



Enter the name and password of an account with permission to join the domain.

Name: TASKSMART\Administrator

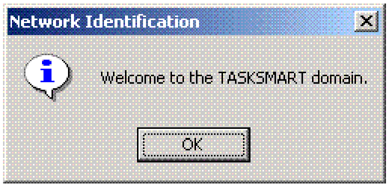
Password: ******

Figure 3-23. Domain Username and Password dialog box

4. Enter the Name in a format identical to that in the example above (DOMAIN NAME\USER NAME). If the domain controller is an Active Directory domain controller, you can enter the user name in the new format (USER@DOMAIN). For example, where the domain name is Tasksmart.Compaq.com, you might enter ADMINISTRATOR@TASKSMART.COMPAQ.COM instead of TASKSMART\Administrator. Typically, the user is a domain administrator, but different users can also be entered.
5. Enter the password.

6. Click **OK**. Adding a computer account to a domain can take several seconds because a new Security ID (SID) is created in the domain for the newly added computer. When the process concludes, a dialog box is displayed. See Figure 3-24.

   NOTE: The name that you assign to the domain is displayed in the dialog box.



Welcome to the TASKSMART domain.

Figure 3-24. Network Identification welcome dialog box

7. Click **OK**. Then close all dialog boxes and restart the server when prompted. The appliance now has a registered computer account in the domain.

Windows NT Server 4.0 Domain—Administering Users and Groups

To administer users and groups in a Windows NT 4.0 domain, use the User Manager for Domains administrative tool. To launch this tool, access the taskbar of any Windows NT 4.0 server on the network. Select **Start**, **Programs**, **Administrative Tools**, **User Manager for Domains**. If User Manager for Domains does not launch directly on the domain controller of the domain to be administered, select **User**, and then **Select Domain.**

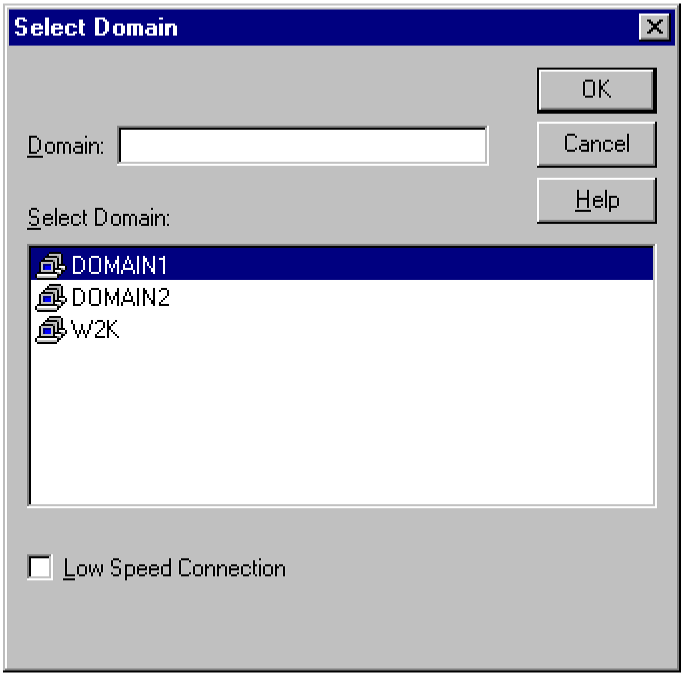


Figure 3-25. Select Domain dialog box, Administering Users and Groups

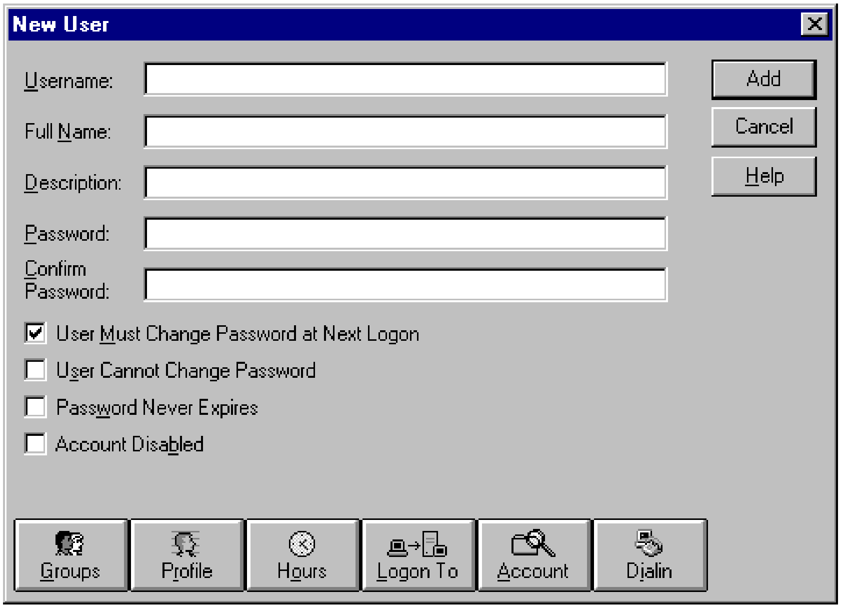
As with Server Manager, type the domain to be administered, or select the domain from the list. Then, configure users and groups.

User Manager for Domains divides users and groups into two windows. The top window lists the users; the bottom window lists the groups. The administration procedure is similar to that for an Active Directory domain.

Windows NT Server 4.0 Domain—Adding a User

The steps that follow describe how to add a new user to the **Windows NT Server 4.0 Domain:**

1. Click **User**, and then click **New User** from the User Manager for Domains menu. The New User dialog box is displayed. See Figure 3-26.



☑ User Must Change Password at Next Logon
☐ User Cannot Change Password
☐ Password Never Expires
☐ Account Disabled

Figure 3-26. New User dialog box,User Manager for Domains manu

2. Enter information into the Username, Full Name, and Description fields.
3. Enter an initial password and confirm it.
4. Select appropriate check boxes to determine the characteristics of the user account. The check boxes are similar to those presented by the Active Directory. See Table 3-4 for an explanation of these characteristics.

Table 3-4
Windows NT Server 4.0 User Account Characteristics

Characteristic	Summary
User must change password at next logon	Checking this box requires the user to change the password at the next logon to the domain.
User cannot change password	If checked, the user cannot modify the password.
Password never expires	If enabled, the domain controller never requires a user to change the password. However, the user can change the password voluntarily.
Account is disabled	If this box is checked, the account is disabled and the user can no longer log on to the domain. However, the account remains on file. If a user forgets a password, failed logon attempts can automatically disable the account. The account can be re-enabled here.

NOTE: As was the case in the Active Directory, users in a Windows NT 4.0 domain typically log on to the domain from their own client machines. Requiring a user to change a password on the first logon proactively addresses security concerns.

Windows NT Server 4.0 Domain—Modifying Group Memberships

By default, the new user is a member of the Domain Users group. The New User dialog box provides configuration choices. To modify the user's group membership, click the first button in the New User dialog box, **Groups.** The Group Memberships dialog box pictured in Figure 3-27 is displayed.

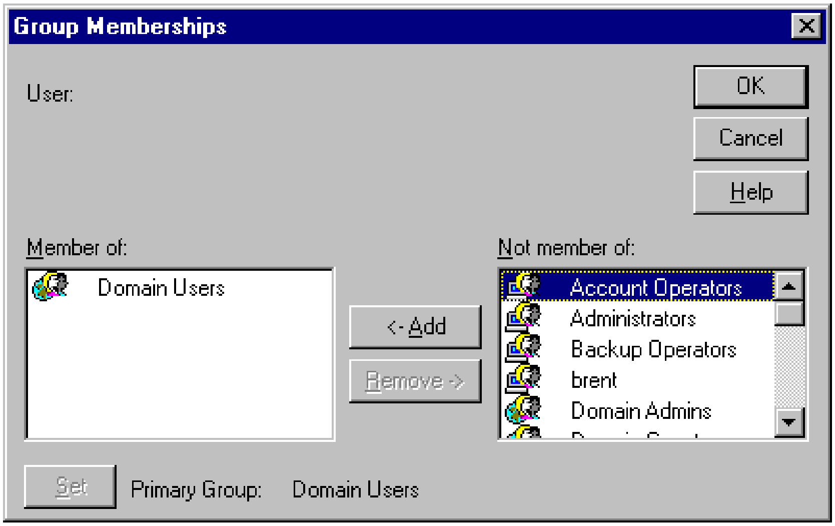


Figure 3-27. Group Memberships dialog box

Complete the following configuration processes to modify a user's group membership:

1. To remove a user's membership, select the desired group or groups from the Member of list, and then click **Remove.** Click **OK** to return to the New User dialog box.
2. To add a user as a member of an additional group, select the desired group or groups from the NOT member of list, and then click **Add**. Click **OK** to return to the New User dialog box.
3. To modify a user's Primary Group membership, select the desired Primary Group, and then click **Set**. Click **OK** to return to the New User dialog box.

Windows NT Server 4.0 Domain—Modifying a User Profile

A user profile can be modified from the New User dialog box by clicking the second button, **Profile**.

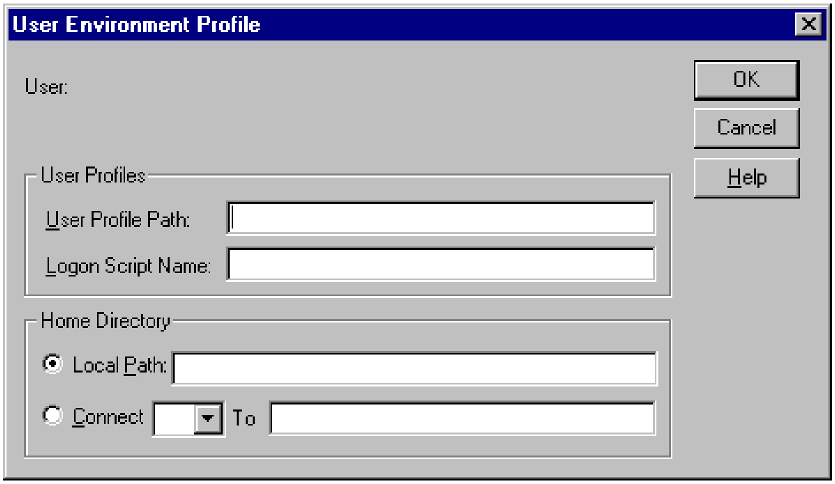


Figure 3-28. User Environment Profile dialog box

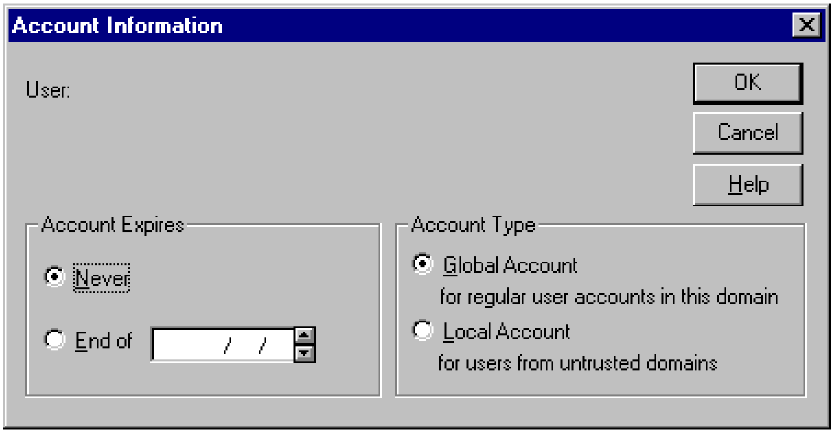
The dialog box configures a user profile path and logon script that launches on the user's client machine anytime the user logs on to the domain. The administrator is responsible for writing the logon script, which can automatically map network drives on the client machine to CIFS shares on the TaskSmart N2400 appliance. The user's Home Directory can also be configured to automatically connect to a CIFS share on the appliance at user logon. When appropriate configuration is complete, click **OK** to return to the New User dialog box.

Click **Help** on the dialog box for more information.

The **Logon To** button on the New User dialog box allows the administrator to restrict the client workstations on which a user can log on to the domain.

The **Account** button on the New User dialog box allows for the configuration of account properties. The following steps describe the process to configure account properties:

1. Click the **Account** button on the New User dialog box.



User:

Account Expires
● Never
○ End of / /

Account Type
● Global Account
for regular user accounts in this domain
○ Local Account
for users from untrusted domains

Figure 3-29. Account Information dialog box

2. Enter an appropriate account expiration date, or leave it at the default setting of Never.

3. Select **Global Account** or **Local Account,** depending on which setting applies. The User Manager for Domains online help, accessible by clicking the Help button, defines Global Account and Local Account as follows:

    - **Global Account—**A global account is a normal user account in the user's home domain. Most accounts are global accounts, which is the default setting. If multiple domains are available, it is best if each user in the network has only one global account in only one domain, so that the user has only one password.

    - **Local Account—**A local account is an account provided in this domain for a user whose regular account is not in a trusted domain. This domain might be a Windows NT server domain that is not trusted by this domain, a LAN Manager domain, or another type of domain or network (User Manager Help).

Selecting Global Account or Local Account depends on the particular network infrastructure in which the domain controller and the appliance are deployed. Select the appropriate option, and then press **OK** to return to the New User dialog box.

The final button, **Dialin,** is described within your Windows NT Server 4.0 documentation. Click **Help** for more details about Dialin.

Windows NT Server 4.0 Domain—Modifying a User

The User Manager for Domains dialog box menu provides several configuration options for modifying users. These options include:

- **Delete a user—**To delete a user from the domain, select the username that you want to delete from the list. Select **User,** and then **Delete** from the User Manager for Domains menu.
- **Modify a username—**To modify a username, select **User,** and then **Rename** from the menu.
- **Modify other user properties—**To modify other user properties, double-click the desired user. A dialog box is launched that is identical to the New User dialog box, except that the username cannot be modified. Refer to the “Windows NT Server 4.0 Domain—Adding a User” section earlier in this chapter for information on how to modify an existing user.

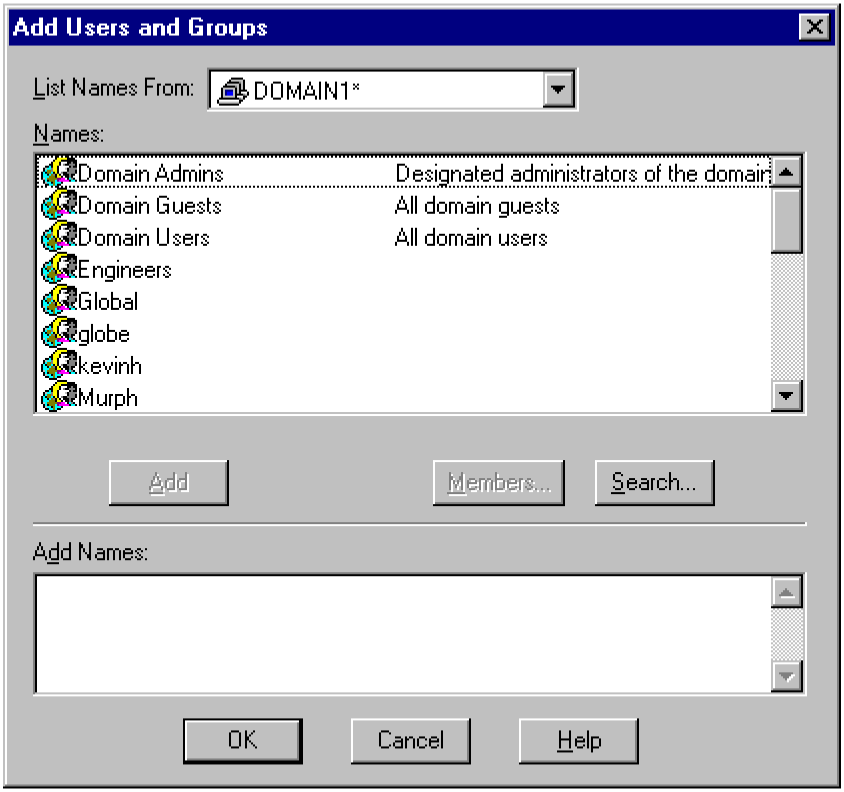
Windows NT Server 4.0 Domain—Local Groups and Global Groups

Just as Local Users and Global Users exist in a Windows NT Server 4.0 domain environment, so also do Local Groups and Global Groups. Refer to the previous definitions of Local and Global accounts for details of each account type.

To create a new Local Group:

1. Click **User** from the User New Local Group menu in the User Manager for the Domains menu.
2. Enter a Group Name and Description.

3. Click **Add** to add users or other groups.



Domain Admins	Designated administrators of the domain
Domain Guests	All domain guests
Domain Users	All domain users
Engineers	
Global	
globe	
kevinh	
Murph	

Figure 3-30. Add Users and Groups dialog box

4. Select the appropriate users and groups.
5. Click **Add** to add them to the list.
6. After the correct users and groups have been added, click **OK.**

When creating new Global Groups, the dialog box illustrated in Figure 3-31 is slightly different from the Local Group dialog box.

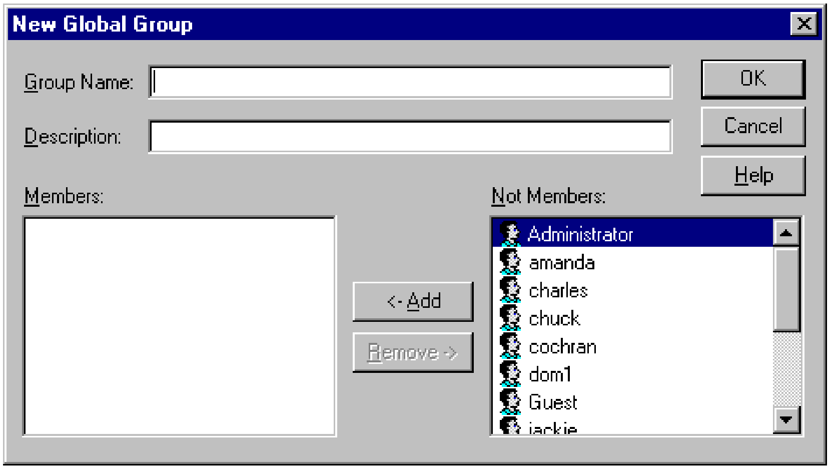


Figure 3-31. New Global Group dialog box

The following steps describe the process used to create a new Global Group:

1. Click **User** from the User New Global Group from the User Manager for the Domains menu.
2. Enter a Group Name.
3. Enter a Description.
4. To add users to this group, select the appropriate entries from the Not Members list and click **Add.**

NOTE: To remove an added user, select the appropriate user from the Members list and click **Remove.**

5. Click **OK** when finished.

After a group has been added, it can be modified or deleted using the User Manager for Domains screen. Follow the process below:

- To delete a group, highlight it on the group list, select **User,** and then **Delete** from the menu.
- To modify a group name, highlight it, press **User,** and then select **Rename** from the menu.
- To change the properties of a group, double-click the desired group.

When a local group is selected, the New Local Group dialog box pictured in Figure 3-32 is displayed.

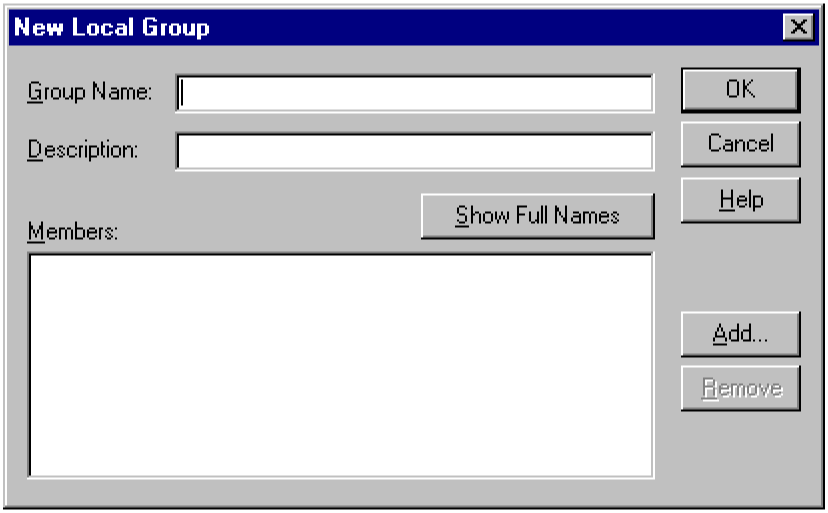
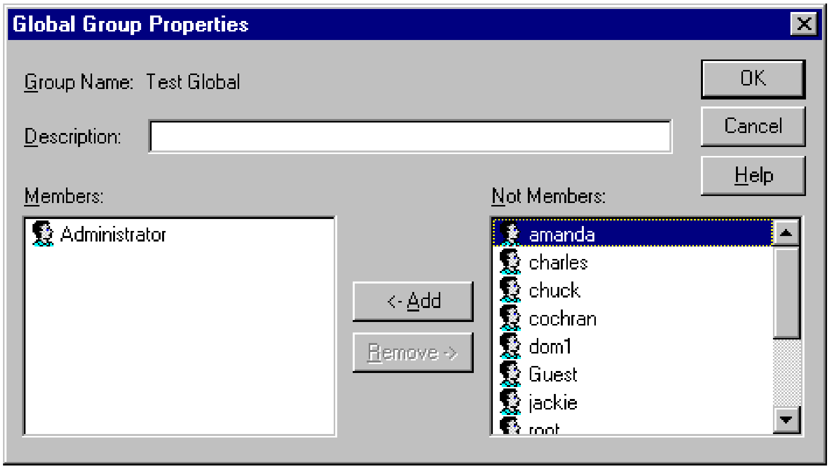


Figure 3-32. New Local Group dialog box

When a global group is selected, the Global Group Properties dialog box is displayed. See Figure 3-33.



Global Group Properties

Group Name: Test Global

Description:

Members:

Administrator

Not Members:

amanda
charles
chuck
cochran
dom1
Guest
jackie
root

Figure 3-33. Global Group Properties dialog box

In both cases, administration is identical to the process for creating a new group.

Managing Group Names

Group management follows many of the same principles as user management.

It is recommended that group naming conventions be systematic and easy to understand. Make the group name convey some logical information about the function or purpose of the group. Table 3-5 provides examples of group names.

Table 3-5
Group Name Examples

Group Name	Description
Administrators	All designated administrators on the server
Users	All standard server users
Power users	All standard server users requiring advanced access levels

Using tags is a helpful convention that indicates the specific access that a particular user has to a network resource. For example, if there is a data share on an appliance, the network administrator can create a “Data Users ROnly” group and a “Data Users RWrite” group to contain users that have read-only or read-write access on the share, respectively.

Windows File System Security

The TaskSmart N2400 appliance uses NTFS Version 5 as the underlying file system. The CIFS network file-sharing protocol uses the file system security model as the basis for its own security model. To effectively administer CIFS shares, it is important to understand the fundamentals of NTFS security. This section documents the relationship between NTFS security and the CIFS file-sharing protocol.

IMPORTANT: CIFS is a network file-sharing protocol that resides on the file system. NTFS is a file system that resides on the drive subsystem, organizing and securing the data written to the drive.

When a CIFS client initiates a request over the network, the request is processed through the appliance CIFS service and is distributed throughout the file system to write the data onto the drive. When data is retrieved from the drive, it is distributed back through the file system and the appliance CIFS service, and then returned to the client.

More information about Windows file system security is available on the Microsoft website:

http://www.microsoft.com/

Access Control Lists

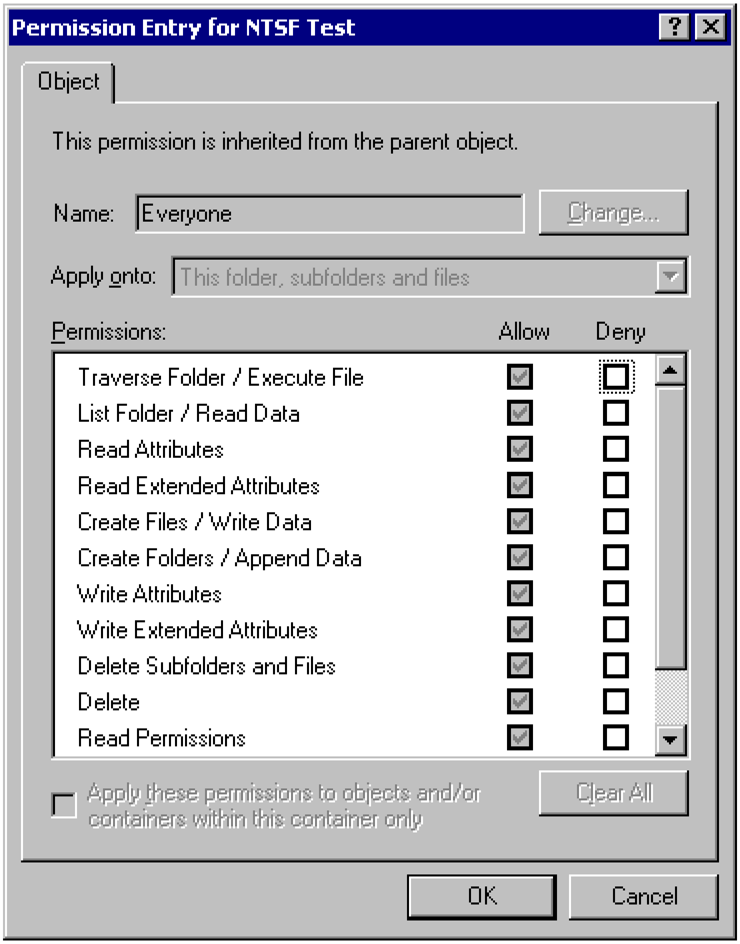
The Access Control List (ACL) contains the information that dictates which users and groups have access to a file, and the type of access that is permitted. Each file on an NTFS file system has one or more ACLs. For example, an ACL can define that User1 has read and write access to a file, User2 has read-only access, and User3 has no access to a particular file. The ACL also includes group access information that applies to every user in a configured group.

Several permissions are available for any file or folder on an NTFS file system. The following steps outline the process used to view these permissions:

1. From either the client machine or the TaskSmart N2400 appliance, open the Windows Explorer interface, and then right-click any NTFS file or folder.
2. Select **Properties.**
3. Select the **Security** tab.
4. Click **Advanced.**

5. From the **Permissions** tab, choose one of the users or groups in the list.
6. Select **View/Edit.** A screen listing of all the available permissions is displayed.

NOTE: Additional permissions are available but are not displayed in Figure 3-34.



This permission is inherited from the parent object.

Name: Everyone

Apply onto: This folder, subfolders and files

Permissions:	Allow	Deny
Traverse Folder / Execute File	☑	☐
List Folder / Read Data	☑	☐
Read Attributes	☑	☐
Read Extended Attributes	☑	☐
Create Files / Write Data	☑	☐
Create Folders / Append Data	☑	☐
Write Attributes	☑	☐
Write Extended Attributes	☑	☐
Delete Subfolders and Files	☑	☐
Delete	☑	☐
Read Permissions	☑	☐

☐ Apply these permissions to objects and/or containers within this container only

Figure 3-34. NTFS File Permission Entry, for file name NTSF Test

It is possible to configure several different combinations of the ACL permissions. Table 3-6 provides descriptions for the available access level permissions.

NOTE: If the permission is not enabled, the access level is denied.

Table 3-6
Access Level Permissions

Permission	Description
Traverse Folder / Execute File	Users can open the folder or execute the file.
List Folder / Read Data	Users can list the contents of a folder or read data from a file.
Read Attributes	Users can read the core attributes from a file or folder (read-only, hidden, archive).
Read Extended Attributes	Users can read the extended attributes from a file or folder (compressed or encrypted).
Create Files / Write Data	Users can create files within a folder or write data to a file.
Create Folders / Append Data	Users can create folders within a folder or append data to an existing file.
Write Attributes	Users can write core attributes to a file.
Write Extended Attributes	Users can write extended attributes to a file.
Delete Subfolders and Files	Users can delete folders and files within a folder.
Delete	Users can delete a file or folder.
Read Permissions	Users can read the permissions for all configured users and groups.
Change Permissions	Users can change permissions for all configured users and groups.
Take Ownership	Users can take ownership of the affected files or folders from another user.

Common access level combinations have logical names that describe the access level. Table 3-7 describes the access level combinations.

Table 3-7
Access Level Description

Access level	Description
Full Control	Allows complete access to all access-level permissions. Includes Modify, Read & Execute, Read, and Write access levels.
Modify	Includes all advanced access properties except: ■ Delete Subfolders and Files ■ Change Permissions ■ Take Ownership
Read & Execute	Includes all advanced access permissions except: ■ Delete Subfolders and Files ■ Delete ■ Change Permissions ■ Take Ownership
List Folder Contents	Includes the following access permissions only: ■ Traverse Folder / Execute File ■ List Folder / Read Data ■ Read Attributes ■ Read Extended Attributes ■ Read Permissions
Read	Includes the following access permissions only: ■ List Folder / Read Data ■ Read Attributes ■ Read Extended Attributes ■ Read Permissions

continued

Table 3-7
Access Level Description *continued*

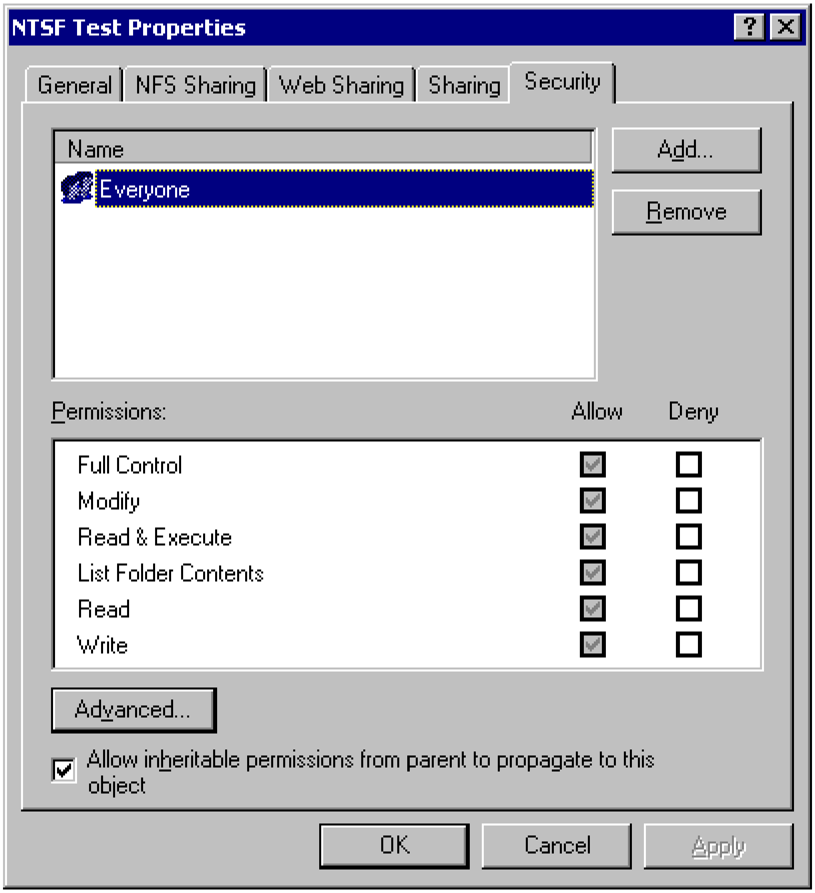
Access level	Description
Write	Includes the following access permissions only: ■ Create Files / Write Data ■ Create Folders / Append Data ■ Write Attributes ■ Write Extended Attributes

NOTE: These access levels can also be combined. For example: Read and Write.

Managing File System Security

File system security can be managed locally by using the TaskSmart N2400 console, or remotely with the Remote Insight Lights-Out Edition board. The necessary steps are outlined below:

1. Place the cursor over a file or folder that you would like to change, and then right-click.
2. Select **Properties.**
3. Click the **Security** tab. Figure 3-35 illustrates the properties available on the Security tab.



Name: Everyone

Permissions:	Allow	Deny
Full Control	☑	☐
Modify	☑	☐
Read & Execute	☑	☐
List Folder Contents	☑	☐
Read	☑	☐
Write	☑	☐

☑ Allow inheritable permissions from parent to propagate to this object

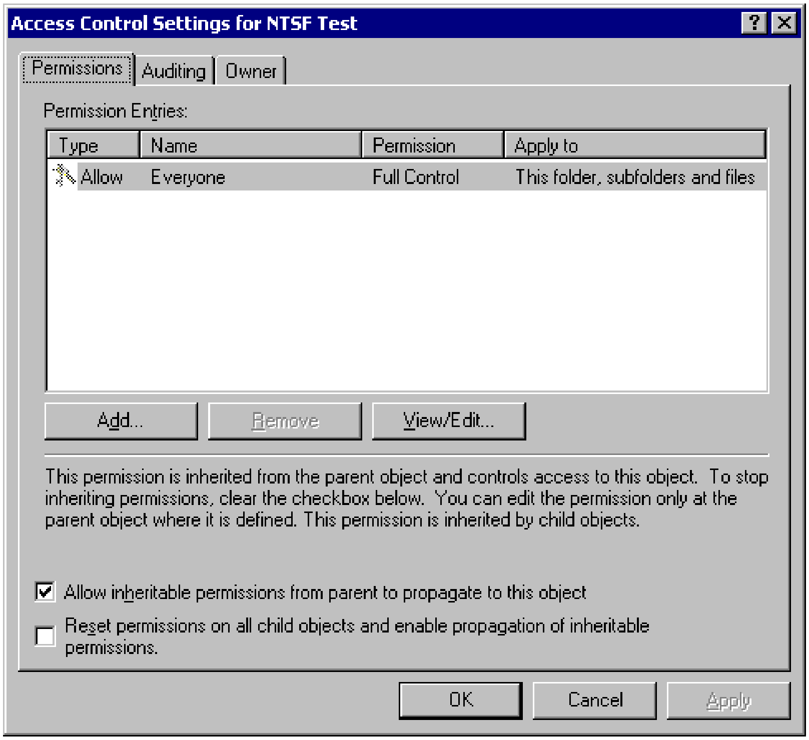
Figure 3-35. Security Properties dialog box for folder name NTSF Test

Several options are available in the Security tab dialog box:

- Add users and groups to the permissions list by clicking the **Add** button. Then follow the dialog box instructions.
- Remove users and groups from the permissions list by highlighting the desired user or group, and then clicking the **Remove** button.
- If the “Allow inheritable permissions from parent to propagate to this object” box at the bottom of the screen is checked, the file or directory inherits permissions from the parent directory. In this case, existing user and group permissions cannot be changed; however, additional users or groups can be added.
- The center section of the Security tab provides a listing of permission levels. When new users or groups are added to the permissions list, select the appropriate boxes to configure the common file access levels.

NOTE: Selections can be made when the “Allow inheritable permissions from parent to propagate to this object” box is disabled.

- The **Advanced** button is used to modify ownership of files or to modify individual file access level permissions. Figure 3-36 illustrates the access control settings screen that is displayed when the **Advanced** button is clicked.



Permission Entries:

Type	Name	Permission	Apply to
Allow	Everyone	Full Control	This folder, subfolders and files

This permission is inherited from the parent object and controls access to this object. To stop inheriting permissions, clear the checkbox below. You can edit the permission only at the parent object where it is defined. This permission is inherited by child objects.

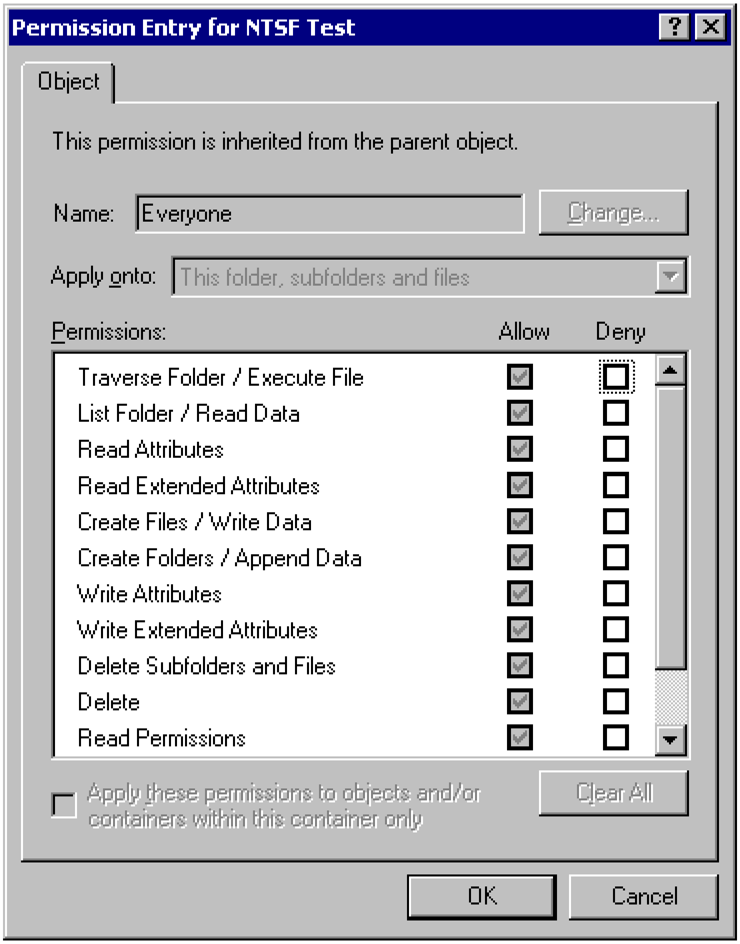
☑ Allow inheritable permissions from parent to propagate to this object

☐ Reset permissions on all child objects and enable propagation of inheritable permissions.

Figure 3-36. Access Control Settings dialog box for folder name NTSF Test, Permissions tab

To modify specific permissions assigned to a particular user or group for a selected file or folder:

1. Select the desired user or group.
2. Click **View/Edit.**
3. Check all the permissions that you want to enable, and clear the permissions that you want to disable. Enable or disable permissions by selecting the Allow box to enable permission or the Deny box to disable permission. If neither box is selected, permission is automatically disabled. Figure 3-37 illustrates the View/Edit screen and some of the permissions.



This permission is inherited from the parent object.

Name: Everyone

Apply onto: This folder, subfolders and files

Permissions:	Allow	Deny
Traverse Folder / Execute File	☑	☐
List Folder / Read Data	☑	☐
Read Attributes	☑	☐
Read Extended Attributes	☑	☐
Create Files / Write Data	☑	☐
Create Folders / Append Data	☑	☐
Write Attributes	☑	☐
Write Extended Attributes	☑	☐
Delete Subfolders and Files	☑	☐
Delete	☑	☐
Read Permissions	☑	☐

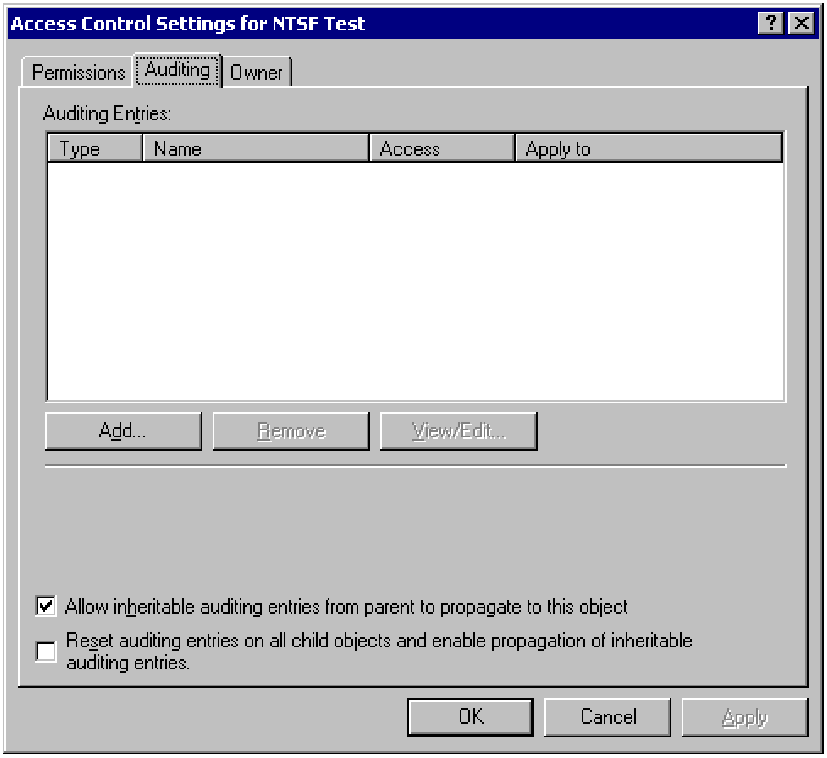
☐ Apply these permissions to objects and/or containers within this container only

Figure 3-37. User or Group Permission Entry dialog box for folder name NTSF Test

Other functionality available in the advanced Access Control Permissions tab is illustrated in Figure 3-36 and includes:

- Add a new user or group. Click **Add,** and then follow the dialog box instructions.
- Remove a user or group. Click **Remove.**
- Inherit permissions from the parent folder. Enable the "Allow inheritable permissions from parent to propagate to this object" box.
- Reset permissions. If the object being configured is a folder, check the "Reset permissions on all child objects and enable propagation of inheritable permissions" box, which allows all child folders and files to inherit the current folder permissions by default.

Another area of the Advanced Access Control is the Auditing tab. Auditing allows you to set rules for the auditing of access, or attempted access, to files or folders. Users or groups can be added, deleted, viewed, or modified through the advanced Access Control Settings Auditing tab. The Auditing tab dialog box is illustrated in Figure 3-38.



☑ Allow inheritable auditing entries from parent to propagate to this object

☐ Reset auditing entries on all child objects and enable propagation of inheritable auditing entries.

Figure 3-38. Access Control Settings, Auditing tab dialog box for folder name NTSF Test

Figure 3-39 illustrates the screen that is displayed when a user or group to be audited is added.

1. Select the appropriate domain or machine name from the “Look in:” drop-down list box at the top of the screen.

   NOTE: A list of users and groups from the desired domain can be viewed if the current user has permission to view the information on the domain.

2. Select the user or group.

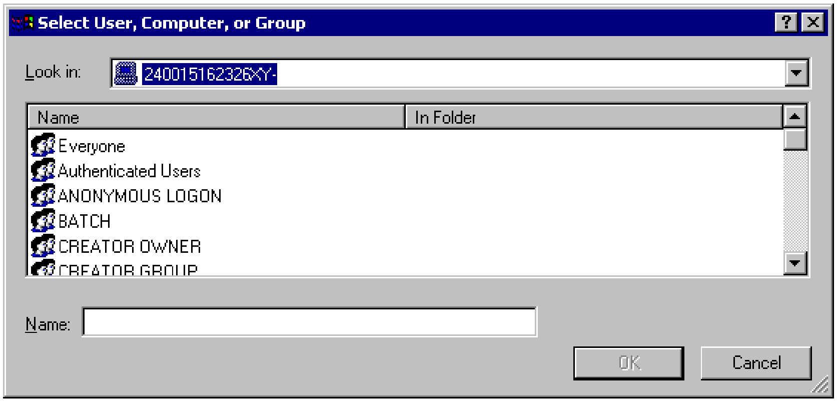
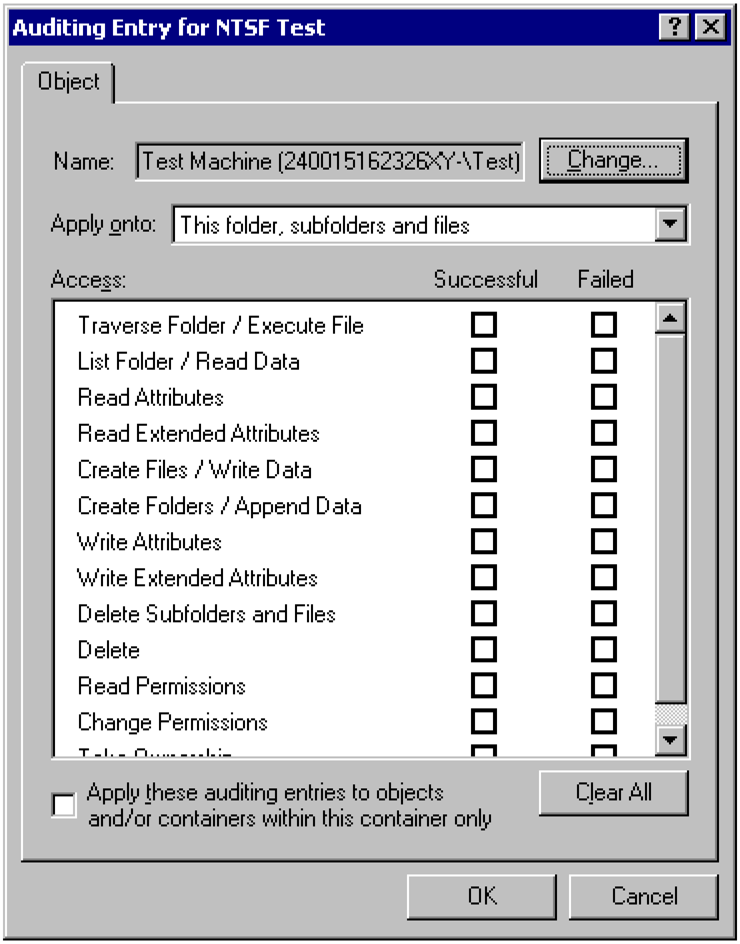


Figure 3-39. Select User, Computer, or Group dialog box

3. Click **OK.** Figure 3-40 illustrates the Auditing Entry screen that is displayed.



Auditing Entry for NTSF Test

Name: Test Machine (240015162326XY-\Test)

Apply onto: This folder, subfolders and files

Access:

	Successful	Failed
Traverse Folder / Execute File	☐	☐
List Folder / Read Data	☐	☐
Read Attributes	☐	☐
Read Extended Attributes	☐	☐
Create Files / Write Data	☐	☐
Create Folders / Append Data	☐	☐
Write Attributes	☐	☐
Write Extended Attributes	☐	☐
Delete Subfolders and Files	☐	☐
Delete	☐	☐
Read Permissions	☐	☐
Change Permissions	☐	☐

☐ Apply these auditing entries to objects and/or containers within this container only

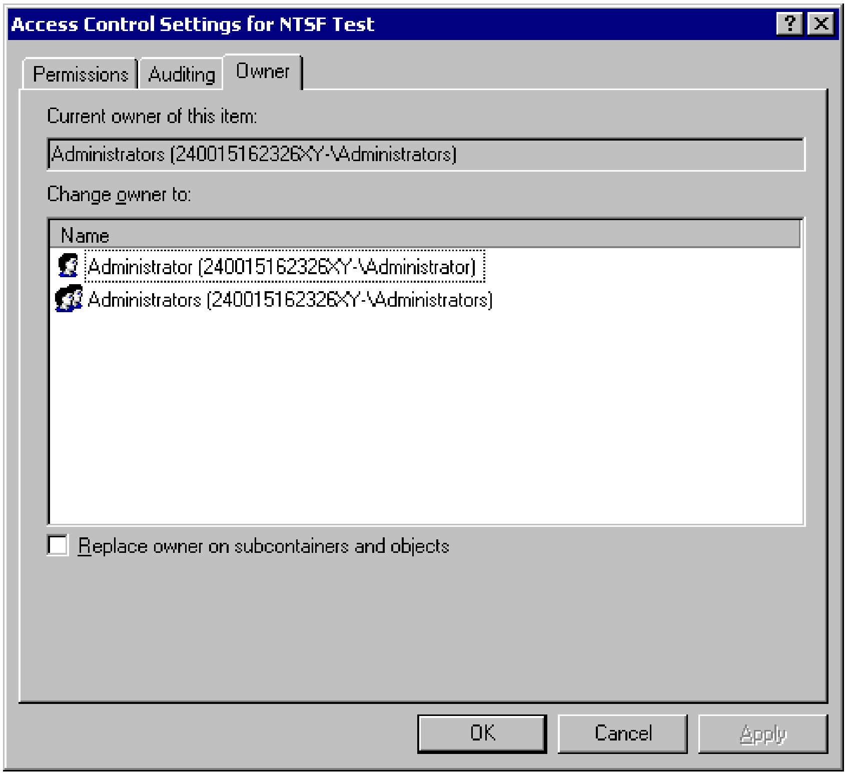
Figure 3-40. Auditing Entry dialog box for folder name NTSF Test

4. Select the desired Successful and Failed audits for the user or group as shown in Figure 3-40.

5. Click **OK**.

NOTE: Auditing must be enabled to configure this information. Use the local Computer Policy Editor to configure the audit policy on the TaskSmart N2400 appliance.

The final tab in the advanced Access Control Settings security configuration is the Owner tab. This tab allows for taking ownership of files. Typically, administrators use this area to take ownership of files when the file ACL is incomplete or corrupt. By taking ownership, you gain access to the files and then manually apply the appropriate security configurations. Figure 3-41 illustrates the Owner tab.



Current owner of this item:
Administrators (240015162326XY-\Administrators)

Change owner to:

Name
Administrator (240015162326XY-\Administrator)
Administrators (240015162326XY-\Administrators)

☐ Replace owner on subcontainers and objects

Figure 3-41. Access Control Settings, Owner tab dialog box for folder name NTSF Test

The current owner of the file or folder is listed at the top of the screen. To take ownership:

1. Select the appropriate user or group from the “Change owner to” list.
2. If it is also necessary to take ownership of subfolders and files, enable the “Replace owner on subcontainers and objects” box.
3. Click **OK** to execute the commands.

Integrating Local File System Security into Windows Domain Environments

All file ACLs include properties specific to users and groups from a particular workgroup server or domain environment. In a multidomain environment, user and group permissions from several domains can apply to files stored on the same appliance. Users and groups local to the TaskSmart N2400 appliance can be given access permissions to files and folders on the appliance. The domain name of the TaskSmart N2400 appliance supplies the context in which the user or group is understood. File level permission configuration depends on the network and domain infrastructure where the appliance resides.

Because the CIFS network file-sharing protocol supplies a user and group context for all connections over the network, appropriate default ACLs are applied to the file system when new files are created. CIFS configuration tools provide the ability to share permissions out to clients. These shared permissions are then propagated into a file system ACL; and when new files are created over the network, the user creating the file becomes the file owner. In cases where a specific subdirectory of a share has different permissions from the share itself, the NTFS permissions on the subdirectory apply instead. This method results in a hierarchical security model where the CIFS network protocol permissions and the file permissions work together to provide appropriate security for CIFS shares on the appliance.

Note the following considerations when CIFS permissions and NTFS file system permissions are stored in the associated ACL of a file:

- CIFS permissions and NTFS file system permissions are implemented separately. It is possible for files on a file system to have different permissions from those applied to a CIFS share. When this situation occurs, the file system permissions override the share permissions. This feature is useful when a single CIFS share is shared out to a large community of users but contains several folders, each with access to a subset of the larger user community.
- The CIFS and NTFS security models are designed to integrate seamlessly. This integration provides the ability for one security model to be applied to the other security model.

CIFS Shares

As noted in the previous discussion about file system permissions and ACLs, the CIFS file security model is based on the NTFS file security model. CIFS file security seamlessly integrates with NTFS file security. This section documents how to manage CIFS shares and discusses CIFS security and other topics.

Setting Up a Share

There are several ways to set up a CIFS share. The first and simplest way is to open a command line interface. Alternatively, CIFS share creation and management can be set up using one of two tools on the TaskSmart N-Series appliance GUI interface.

Setting Up a Share Using the Command Line Interface

The simplest way to set up a CIFS share is to open a command line interface to the TaskSmart N-Series server and type:

```
NET SHARE <share name>=<full path to folder>
```

For a command line interface, click **Command Prompt** on the GUI or connect to the appliance through Telnet Server from a remote client.

For further help on the NET SHARE command, type NET HELP SHARE. The full text output of NET HELP SHARE follows:

```
NET SHARE sharename

      sharename=drive:path [/USERS:number | /UNLIMITED]

                 [/REMARK:"text"]

                 [/CACHE:Manual | Automatic | No ]

      sharename [/USERS:number | /UNLIMITED]

                 [/REMARK:"text"]

                 [/CACHE:Manual | Automatic | No ]

      {sharename | devicename | drive:path} /DELETE
```

The NET SHARE command makes CIFS server resources available to network users. When used without options, it lists information about all resources being shared on the computer. For each resource, Windows reports the device name or names, or path name or names, and an associated descriptive comment.

Table 3-8
NET SHARE Resources

Device Name/Path Name	Description
Sharename	Provides the network name of the shared resource. To see information about the share, type **NET SHARE** with the sharename only
drive:path	Specifies the absolute path of the directory to be shared
/USERS:number	Sets the maximum number of users who can simultaneously access the shared resource
/UNLIMITED	Specifies an unlimited number of users who can simultaneously access the shared resource
/REMARK:"text"	Adds a descriptive comment about the resource and encloses the text in quotation marks
/DELETE	Stops sharing the resource
/CACHE:Automatic	Enables offline client caching with automatic reintegration
/CACHE:Manual	Enables offline client caching with manual reintegration
/CACHE:No	Advises client that offline caching is inappropriate

Setting Up a Share using the Microsoft Management Console (MMC)

To invoke the MMC snap-in necessary to administer CIFS shares:

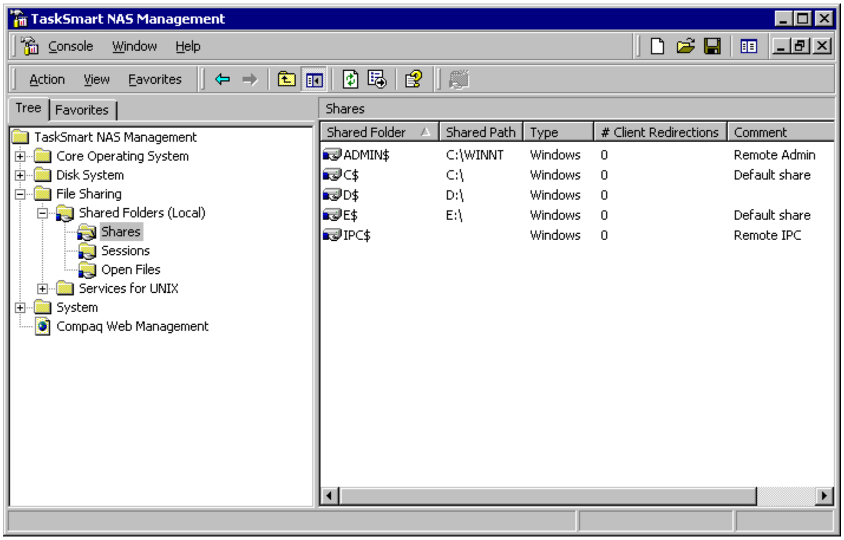
1. From the TaskSmart N-Series console, click **Microsoft Management Console.** This request invokes the MMC that includes several useful snap-ins.
2. Navigate to the File Sharing folder.
3. Open the Shared Folders subfolder.

NOTE: You can also administer CIFS shares through remote MMC by pointing the remote Shared Folders snap-in on a client machine to the TaskSmart N2400 appliance. Either way, three subfolders are displayed.

Table 3-9
MMC Subfolders

Subfolder Name	Description
Shares	Lists all CIFS shares on the appliance, including administrative shares. Shares can be added, removed, or modified in this subfolder. See the “Administrative Compared to Standard Shares” section at the end of this chapter for details.
Sessions	Lists all current client sessions connected to the appliance. Client sessions can be managed in this subfolder.
Open Files	Lists all files currently open through CIFS from the appliance. Open files can be managed in this subfolder.

The full MMC console for file sharing administration is illustrated in Figure 3-42. All the file shares, including administrative shares, are listed along with summary data for each share.

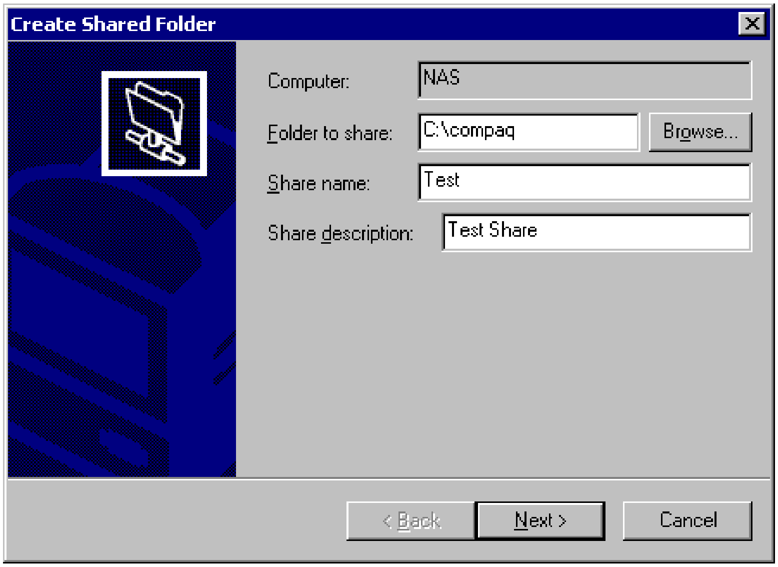


Shared Folder	Shared Path	Type	# Client Redirections	Comment
ADMIN$	C:\WINNT	Windows	0	Remote Admin
C$	C:\	Windows	0	Default share
D$	D:\	Windows	0	
E$	E:\	Windows	0	Default share
IPC$		Windows	0	Remote IPC

Figure 3-42. TaskSmart NAS Management MMC consol for file sharing administration

The administrator is allowed to create, delete, and modify shares from the MMC console. The following steps outline how to create a share using the MMC console:

1. On the **Action** menu, select **New File Share**.

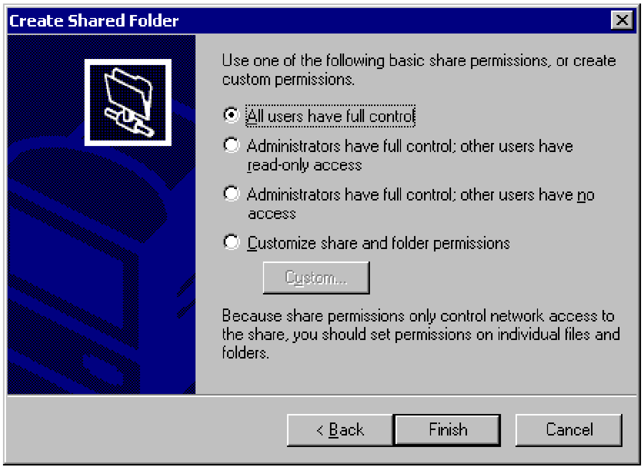


Computer: NAS
Folder to share: C:\compaq
Share name: Test
Share description: Test Share

Figure 3-43. Create Shared Folder dialog box

2. Enter the appropriate information for Folder to share, browsing for a particular folder if necessary.
3. Enter Share name and a comment to describe the share.

4. Click **Next.** The dialog box illustrated in Figure 3-44 is displayed.



Create Shared Folder

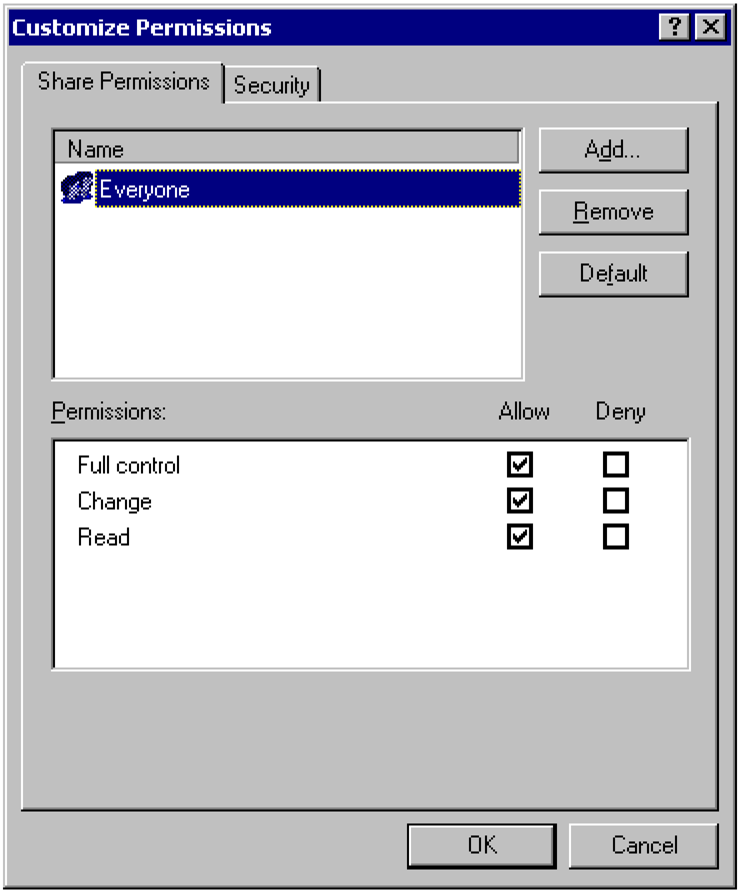
Use one of the following basic share permissions, or create custom permissions.

- ● All users have full control
- ○ Administrators have full control; other users have read-only access
- ○ Administrators have full control; other users have no access
- ○ Customize share and folder permissions

Because share permissions only control network access to the share, you should set permissions on individual files and folders.

Figure 3-44. Create Shared Folder dialog box, customizing

5. Select the appropriate permissions level. If a custom permissions level is desired, select the "Customize share and folder permissions" option button, and then click **Custom.**



Name
Everyone

Permissions:	Allow	Deny
Full control	☑	☐
Change	☑	☐
Read	☑	☐

Figure 3-45. Customize Permissions dialog box, Share Permissions tab

Share permissions are managed using a dialog box similar to the dialog box used for managing NTFS file permissions. There are three permission levels: Read, Change, and Full Control. Each permission level allows connected users specific capabilities with the files located in the share. The following list describes each permission level in detail.

- The Read permission level allows:
  - Viewing file names and subfolder names
  - Traversing to subfolders
  - Viewing data in files
  - Running program files

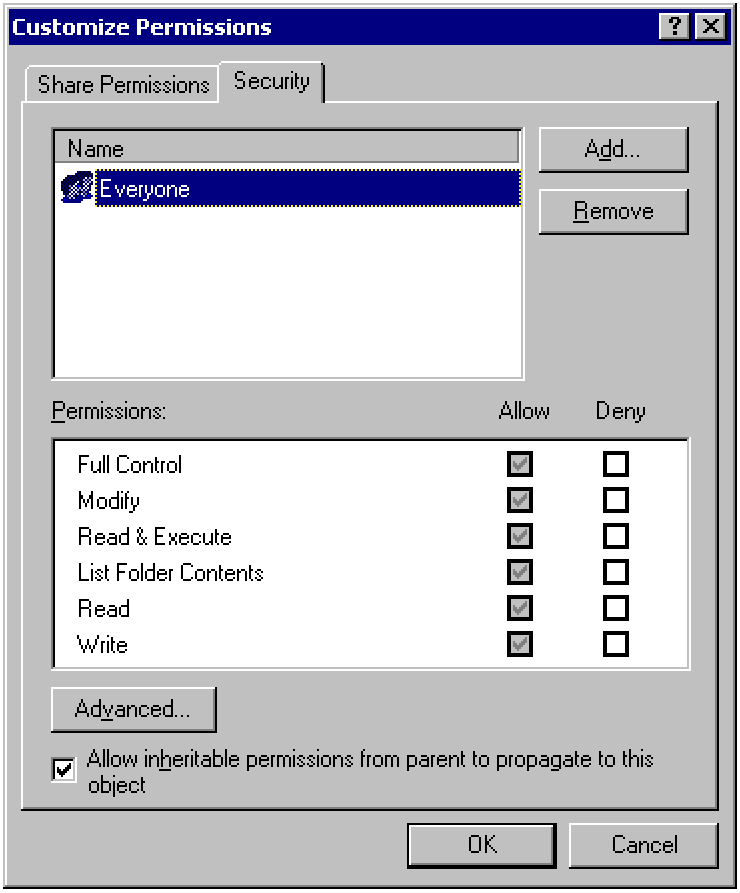
- The Change permission level allows all Read permissions, plus:
    - Adding files and subfolders
    - Changing data in files
    - Deleting subfolders and files
- Full Control is the default permission applied to any new shares that you create. It allows all Read and Change permissions, plus for NTFS files and folders only::
    - Changing permissions
    - Taking ownership (MMC help for the Shared Folders snap-in)

Any of these access permission levels can be applied to shared folders. Choose an appropriate permissions level for each user or group configured to have access to the share.

> **NOTE:** If a subfolder has a different level of permissions applied to it at the file system level, the file system permissions apply. This control allows administrators to build a hierarchical security model into their file-sharing strategy.

> **NOTE:** The dialog box for adding users or groups to the share permissions list is identical to the dialog box for adding users or groups to a directory permissions list.

The second tab on the Customize Permissions property page deals with share security. The Security tab is illustrated in Figure 3-46.



Name
Everyone

Permissions:	Allow	Deny
Full Control	☑	☐
Modify	☑	☐
Read & Execute	☑	☐
List Folder Contents	☑	☐
Read	☑	☐
Write	☑	☐

☑ Allow inheritable permissions from parent to propagate to this object

Figure 3-46. Customize Permissions dialog box, Security tab

The Security tab allows you to edit the file system security properties that apply to the share folder on the appliance. This information is administered in the same way security settings are administered for files and folders on the NTFS file system. See “Windows File System Security” earlier in this chapter for more information.

After appropriate permissions and file system security properties have been set for the share, click **OK** to return to the Create Share Wizard dialog box. Click **Finish** to create the share.

Deleting a Share Using the MMC

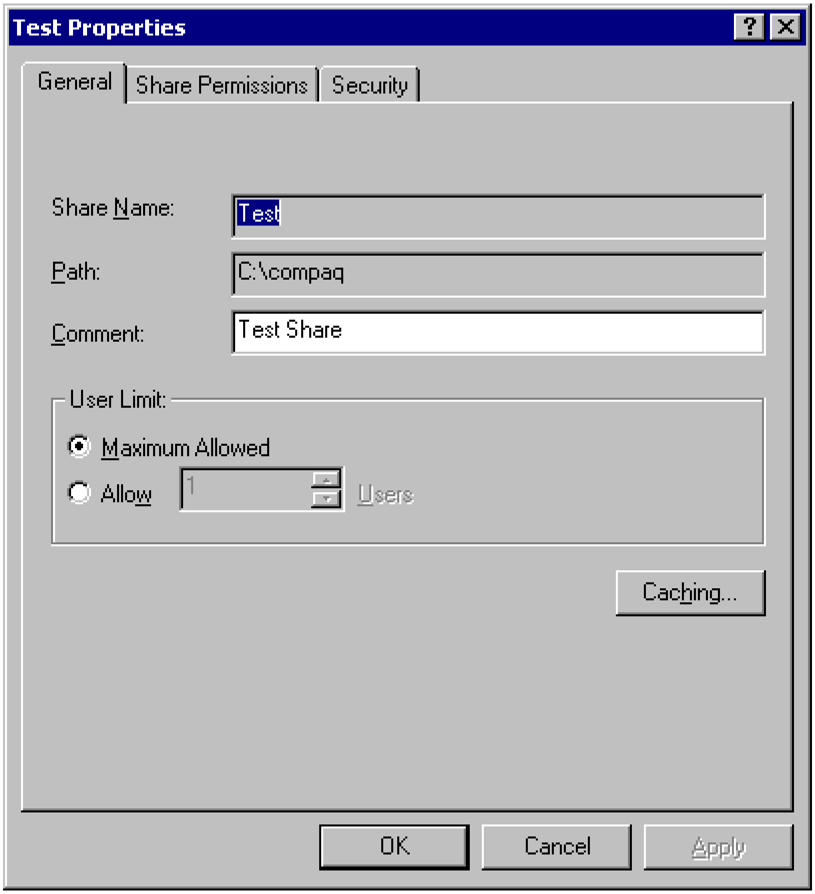
To delete a share using the MMC:

1. From the MMC console, highlight the share that you want to delete.
2. Select **Action,** and then **Stop Sharing.**

Modifying a Share Using the MMC

To modify any share through the MMC interface:

1. From the MMC, select the share that you want to modify.
2. Select **Action,** and then **Properties**.



Share Name: Test

Path: C:\compaq

Comment: Test Share

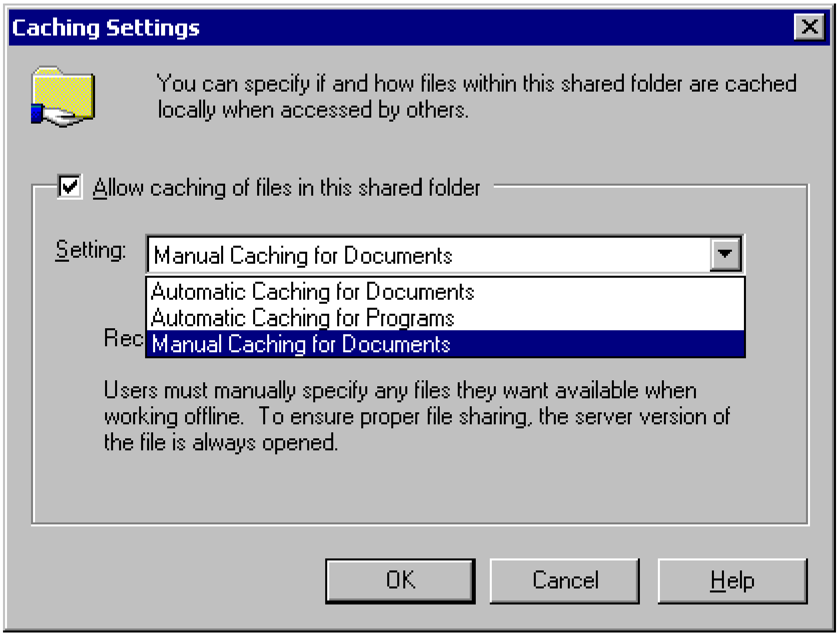
● Maximum Allowed

○ Allow 1 Users

Figure 3-47. Share Properties dialog box, General tab

The Share Permissions and Security tabs are identical to the dialog boxes that allow for setting custom permissions when the share is created. The General tab allows three properties to be modified: comment, user limit, and caching.

3. Modify the comment by highlighting the text area and typing a comment that appropriately describes the share.
4. Modify the user limit to restrict the number of users who can access the share at any given time by clicking the **Allow** option button. Then, select the desired number of users.
5. Click **Caching** to set up caching settings. Figure 3-48 illustrates the dialog box that is displayed.



Caching Settings

You can specify if and how files within this shared folder are cached locally when accessed by others.

☑ Allow caching of files in this shared folder

Setting: Manual Caching for Documents

Rec

Users must manually specify any files they want available when working offline. To ensure proper file sharing, the server version of the file is always opened.

Automatic Caching for Documents
Automatic Caching for Programs
Manual Caching for Documents
OK
Cancel
Help

Figure 3-48. Caching Settings dialog box

The default caching is Manual Caching for Documents. Other settings include Automatic Caching for Documents and Automatic Caching for Programs. Table 3-10 describes each caching setting.

Table 3-10
Caching Settings

Setting	Description
Manual Caching for Documents	Default setting. Recommended for folders containing user documents. Users must manually specify any files that they want available when working offline. To ensure proper file sharing, the server version of the file is always open.
Automatic Caching for Documents	Recommended for folders containing user documents. Open files are automatically downloaded and made available when working offline. Older copies are automatically deleted to make room for newer, more recently accessed files. To ensure proper file sharing, the server version of the file is always open.
Automatic Caching for Programs	Recommended for folders with read-only data, or run-from-the-network applications. File sharing is not ensured. Open files are automatically downloaded and made available when working offline. Older copies are automatically deleted to make room for newer, more recently accessed files.

6. When modifications are complete, click **OK** to return to the Share Properties dialog box.
7. After modifying share properties, click **OK** to apply the modifications.

Managing CIFS Sessions Using MMC

In addition to managing file shares, the MMC provides tools for managing CIFS sessions. Figure 3-49 illustrates the CIFS Shared Folders Session Manager.

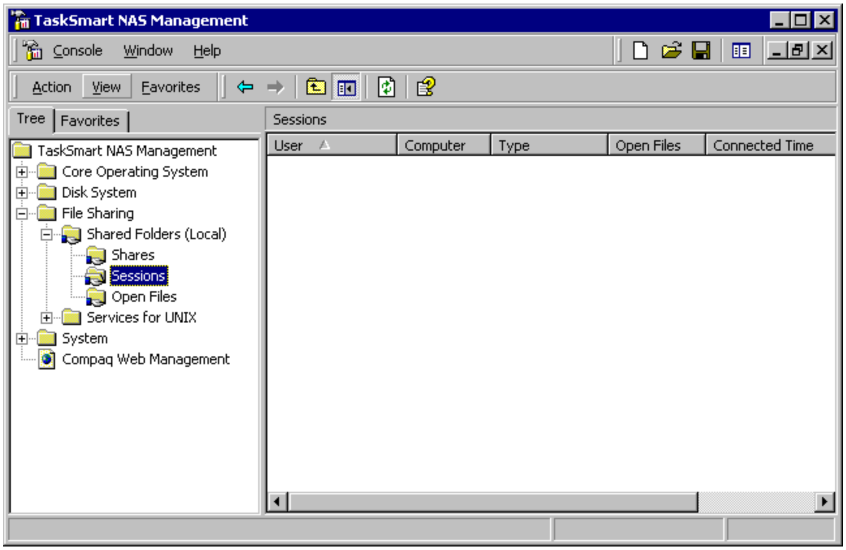


Figure 3-49. TaskSmart NAS Management dialog box, CIFS Session manager using MMC

All CIFS sessions that are open on the server, including information about the user and client that initiated the session, are displayed in the CIFS Session Manager.

To terminate a specific session:

1. Highlight the session.
2. Select **Action,** and then **Close Session.**

For security and maintenance reasons, it is sometimes necessary to forcibly disconnect client sessions. To disconnect all sessions:

1. Deselect all highlighted sessions.
2. Select **Action**, and then click **Disconnect All Sessions.**

CAUTION: Disconnecting a session forces the currently connected user, or users, to disconnect their CIFS sessions from the server. As a result, it is possible that data loss could occur.

Managing CIFS Open Files Using MMC

The final tool that the MMC provides is CIFS open file management. Figure 3-50 illustrates the MMC CIFS Open Files screen. This screen lists all files currently open by CIFS clients, including information about the particular file or folder, the user accessing the client, the number of locks, and the read mode. This tool is useful in managing because an administrator can close any open files through this interface.

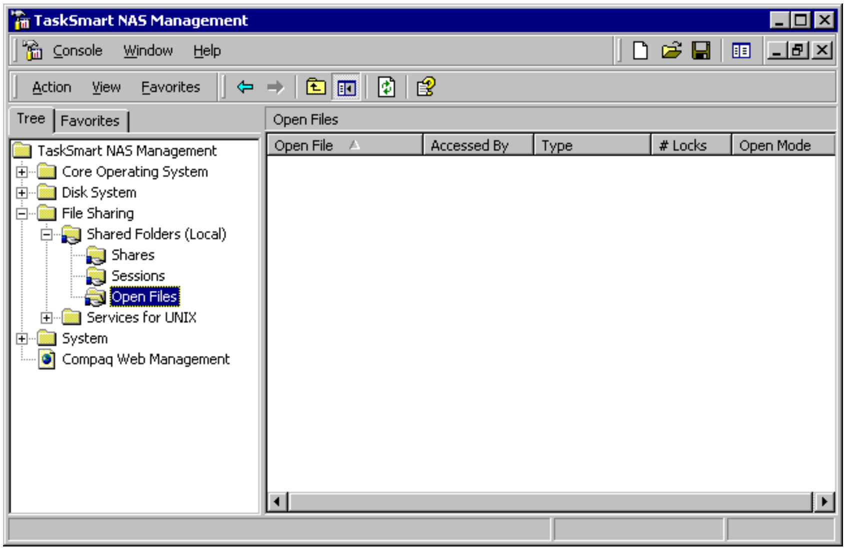


Figure 3-50. TaskSmart NAS Management dialog box, Open Files manager using MMC

To close a single open file:

1. Highlight the file that you want to close.
2. Click **Action,** and then **Close Open File.**

To close all open files:

1. Deselect all the files from the list.
2. Click **Action,** and then click **Disconnect All Open Files.**

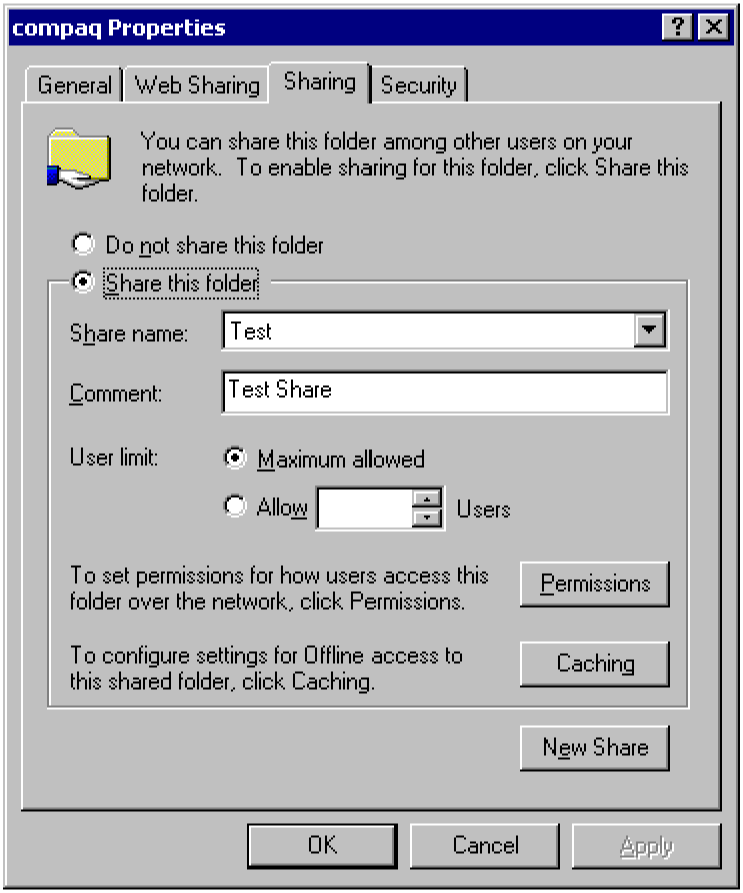
△ **CAUTION:** Disconnecting all the open files forcibly closes all files that CIFS users currently have open. Data loss can occur when users are editing affected files.

Windows Explorer

CIFS shares can also be administered directly through the Windows Explorer interface on the appliance.

Setting Up a CIFS Share Using Windows Explorer

1. Right-click on the folder that you wish to share.
2. Select **Sharing**. Figure 3-51 illustrates the dialog box that is displayed.



You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: Test

Comment: Test Share

User limit: ● Maximum allowed

○ Allow Users

To set permissions for how users access this folder over the network, click Permissions.

To configure settings for Offline access to this shared folder, click Caching.

Figure 3-51. UserData Properties dialog box, Sharing tab

3. Click the “Share this folder” option button to share the folder.

NOTE: The folder name is inserted as the share name by default. If not, then a share with the same name as the folder already exists.

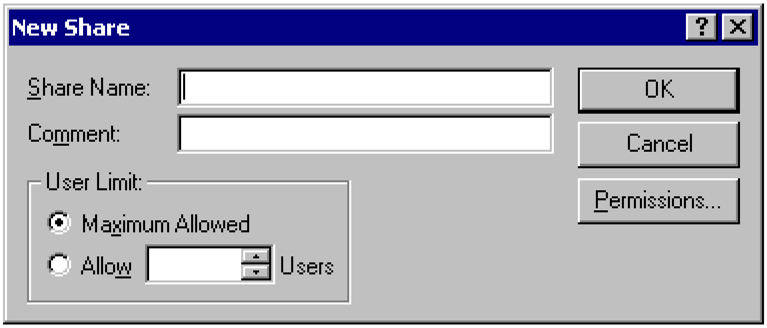
4. Select an appropriate User Limit.
5. Click **Permissions**, then assign the appropriate values.
6. Click **Caching** to set up caching settings.

NOTE: Refer to the “Modifying a Share Using the MMC” section earlier in this chapter for assistance in the administration of user limits, permissions, or caching.

7. Click **OK** to apply all share properties.

The New Share button allows you to share the same folder with a different name. Use the following instructions to add a different name to the existing share:

1. Click **New Share.** Figure 3-52 illustrates the dialog box that is displayed.



User Limit:
● Maximum Allowed
○ Allow Users

Figure 3-52. New Share dialog box

2. Type the share name in the **Share Name** text box.
3. Type a comment in the **Comment** text box.
4. Type an appropriate user limit.

5. Click **Permissions** to apply different permissions to the new share name.

   NOTE: This feature can be used to ensure compatibility between NFS and CIFS shares with spaces in their names. It can also be shared without the space so that at least one CIFS share name is identical to the NFS export name for the same folder. This feature is also useful for providing a different security model on the same data.

6. Click **OK** to return to the share properties dialog box.
7. Click **OK** to apply all changes.

Deleting a CIFS Share Using Windows Explorer

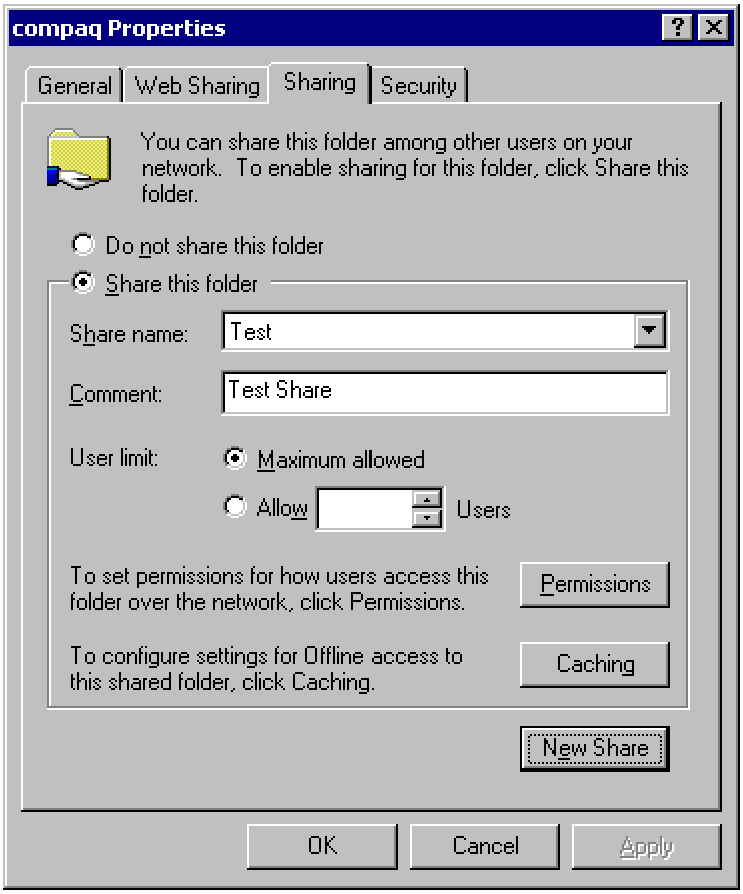
To delete a CIFS share through the Windows Explorer interface:

1. Right-click on the shared folder.
2. Select **Sharing**.
3. Select the **Do not share this folder** option button.
4. Click **OK**.

Modifying a CIFS Share Using Windows Explorer

To modify a CIFS share through the Windows Explorer interface:

1. Right-click the shared folder.
2. Select **Sharing**. Figure 3-53 illustrates the dialog box that is displayed.



compaq Properties

You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: Test

Comment: Test Share

User limit: ● Maximum allowed

○ Allow Users

To set permissions for how users access this folder over the network, click Permissions.

To configure settings for Offline access to this shared folder, click Caching.

Figure 3-53. UserData Properties dialog box, Sharing tab

3. Select an appropriate User Limit.
4. Click **Permissions**, and then assign the appropriate values.
5. Click **Caching** to set up caching settings.

Administrative Compared to Standard Shares

CIFS supports both administrative shares and standard shares. **Administrative** shares are shares with a last character of “$”. Administrative shares are not included in the list of shares when a client browses for available shares on a CIFS server. **Standard** shares are shares that do not end in a “$” character. Standard shares are listed whenever a CIFS client browses for available shares on a CIFS server.

The TaskSmart N2400 appliance supports both administrative and standard CIFS shares. To create an administrative share, end the share name with the “$” character when setting up the share. To create a standard share, do not type a “$” character at the end of the share name.

Planning for Compatibility Between CIFS and NFS

When you plan for cross-platform share management on the TaskSmart N2400 appliance, it is important to remember two considerations.

Consider the following two administrative requirements to provide the greatest compatibility between CIFS and NFS. Further information, including details about the NFS Service and the User Mapping service, is available in “User Name Mapping” in Chapter 4, “Integrating UNIX into Windows NT.”

- NFS service does not support spaces in the names for NFS exports.

  NFS translates any spaces in an export into an underscore character. Additional translations can be set up for files. See the Compaq “OEM Supplemental Help” chapter of the SFU help, found on the TaskSmart N2400 console. This feature is designed to ensure the greatest level of compatibility with NFS clients, because some do not work with NFS exports that contain a space in the export name. If you plan to use the same name when sharing a folder through CIFS, and then exporting it through NFS, do not put spaces in the CIFS share name.

- NFS service does not support exporting a child folder when its parent folder has already been exported.

The child folder can be accessed by selecting the parent folder on an NFS client and navigating to the child folder. If strict cross-platform compatibility is an administration goal, CIFS must be managed in the same way. Do not share a folder through CIFS if the parent folder is already shared.

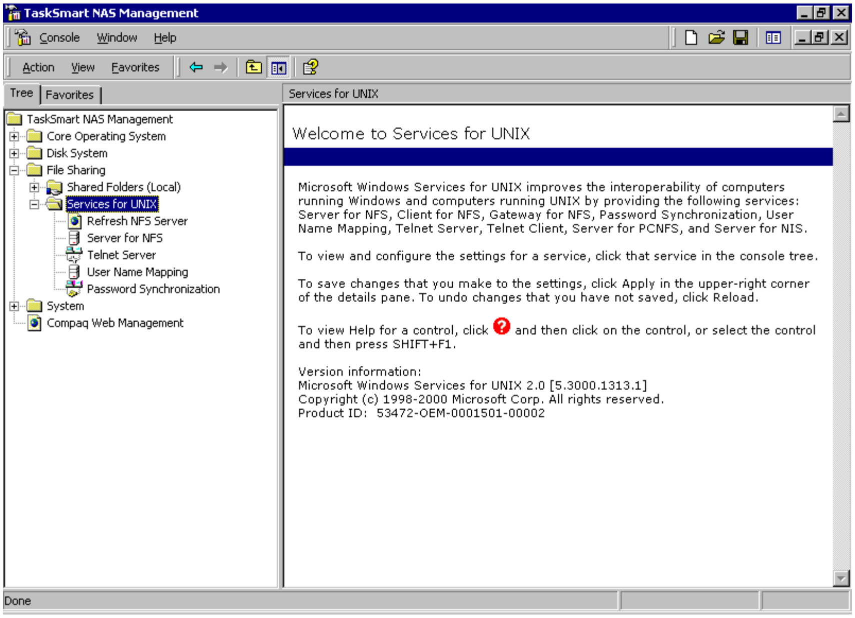
One exception to this rule applies to administrative shares. Unless the entire drive at the drive-letter level is intended for export through NFS, the administrative shares can stay in place. However, if an entire drive is intended for export through NFS, the administrative share, “F$” for example, must be replaced with a CIFS share name that corresponds to the name of the NFS export. Thus, if the F:\ drive is exported through NFS as /FDrive, the administrative CIFS share F$ must be changed to a standard CIFS share named FDrive.

Chapter 4

Integrating UNIX into Windows NT

Microsoft Services for UNIX

Microsoft Services for UNIX (SFU) is a comprehensive software package designed to provide complete UNIX environment integration of a Windows NT file server.



Welcome to Services for UNIX

Microsoft Windows Services for UNIX improves the interoperability of computers running Windows and computers running UNIX by providing the following services: Server for NFS, Client for NFS, Gateway for NFS, Password Synchronization, User Name Mapping, Telnet Server, Telnet Client, Server for PCNFS, and Server for NIS.

To view and configure the settings for a service, click that service in the console tree.

To save changes that you make to the settings, click Apply in the upper-right corner of the details pane. To undo changes that you have not saved, click Reload.

To view Help for a control, click ❓ and then click on the control, or select the control and then press SHIFT+F1.

Version information:
Microsoft Windows Services for UNIX 2.0 [5.3000.1313.1]
Copyright (c) 1998-2000 Microsoft Corp. All rights reserved.
Product ID: 53472-OEM-0001501-00002

Figure 4-1. SFU screen user interface

The following SFU components are described in this section:

- Network File System (NFS)
- Server for NFS
- User Name Mapping
- Mortice Kern Systems (MKS) Toolkit

Network File System

Network File System (NFS) is a networking protocol for exporting UNIX file systems across a network.

There are three key design goals of NFS:

1. Allow different UNIX machines to transparently export files across a network

   This feature works across different versions of UNIX and across different platforms. For example, a Linux machine can access files on a *Tru64*™ UNIX machine. Accessing these files is transparent to both the administrator and the users. The administrator and user do not notice any difference between accessing local files or files on the remote machine.

2. Make the administration as easy as possible

   The remote file system connects to the local machine in the same manner that a local file system does. The administrator is able to add a remote file system in the same manner as adding another hard drive or external storage.

3. Focus exclusively on file system operations

   The file system is used only for exporting file systems to remote machines. NFS supports only operations such as read, write, create, delete, and copy.

NFS Configurations

There are two versions of NFS, Version 2 and Version 3. Version 3 supports additional file operations that Version 2 did not have, such as asynchronous file operations.

NFS has the capacity to operate with two different network protocols:

- Transport Control Protocol (TCP)
- User Datagram Protocol (UDP)

Traditionally, NFS operates with UDP for performance purposes, but it can also operate with TCP. This operating ability allows for four possible combinations:

- NFS Version 2 operating with UDP
- NFS Version 2 operating with TCP
- NFS Version 3 operating with UDP
- NFS Version 3 operating with TCP

Authentication

NFS export access is granted or denied to clients based on client name or IP address. The server determines whether or not a specific client machine has access to an NFS export. No user logon to the NFS server takes place when a file system is exported by the NFS server. Permission to read or write to the export is granted to specific client machines. For example, if client machine M1 is granted access to an export but client M2 is not, user jdoe can access the export from M1 but not from M2.

The permissions are on a per-export basis. That means that each export has its own permissions, independent of other exports on the system. For example, file system *a* can be exported to allow only the Accounting department access, and file system *m* can be exported allowing only the Management department access. If a user in Management needs access to the Accounting information, the *a* export permissions can be modified to let that one user’s client machine have access. This modification does not affect other client access to the same export, nor does it allow the Management user or client access to other exports.

After the client machine has permission to the export, the user logon affects file access. The client machine presents the UNIX user's user ID (UID) and group ID (GID) to the server. When the computer accesses a file, the user logon is compared against the typical UNIX permissions of “user,” “group,” and “other,” and typical UNIX access is applied.

NOTE: User credentials are not questioned or verified by the NFS server. The server accepts the presented credentials as valid and correct.

If the NFS server does not have a corresponding UID or GID, or if the administrator has set other conditions to filter out the user, a process called “squashing” takes effect. Squashing is the conversion of an unknown or filtered user to an “anonymous” user. This anonymous user has very restricted permissions on the system. Squashing helps administrators manage access to their exports by allowing them to restrict access to certain individuals or groups and to squash all others down to restricted (or no) access. Squashing enables the administrator to allow permissions instead of denying access to all the individuals who are not supposed to have access. See the section titled “User Name Mapping” later in this chapter for more details.

Server for NFS

The SFU NFS server provides native file system support for NFS. Windows NT files can be exported and accessed through NFS.

Until recently, UNIX used only NFS to export files. UNIX was not able to share files with Windows platforms, and Windows platforms were not able to share files with UNIX.

This restriction caused UNIX clients to require UNIX file servers, and Windows clients to require Windows file servers. Windows platforms and UNIX were totally separate environments, including the duplication of hardware, overhead, and effort.

SFU enables UNIX clients to use Windows-based machines as file servers. The SFU NFS server supports NFS Version 2 and Version 3, and supports them both on the TCP and UDP network protocols.

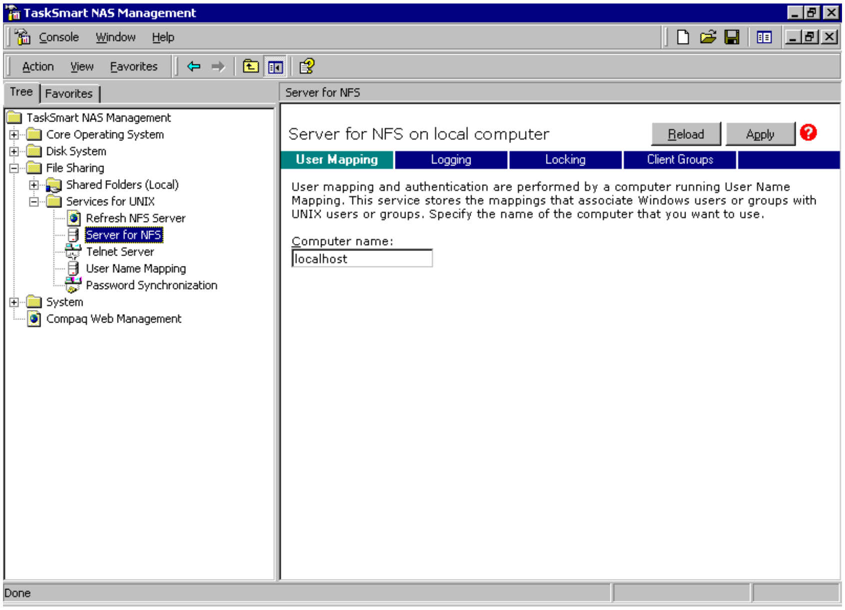
SFU is more fully integrated into the operating system than other third-party NFS server packages. The administrative interface for NFS exports is similar to the Common Internet File System (CIFS) sharing interface used by Windows platforms.

Implementation

1. In the Services for UNIX folder, click **Server for NFS.**
2. In the Computer name box on the user mapping screen, type the name of the computer designated for user mapping and authentication.
3. To run user mapping on the TaskSmart N2400 appliance, type localhost.

NOTE: Localhost is the computer name assigned by default on the TaskSmart N2400 appliance.

4. If a machine other than the local host is to be used, make sure that the user name mapping service is installed and running on that machine.



Server for NFS on local computer

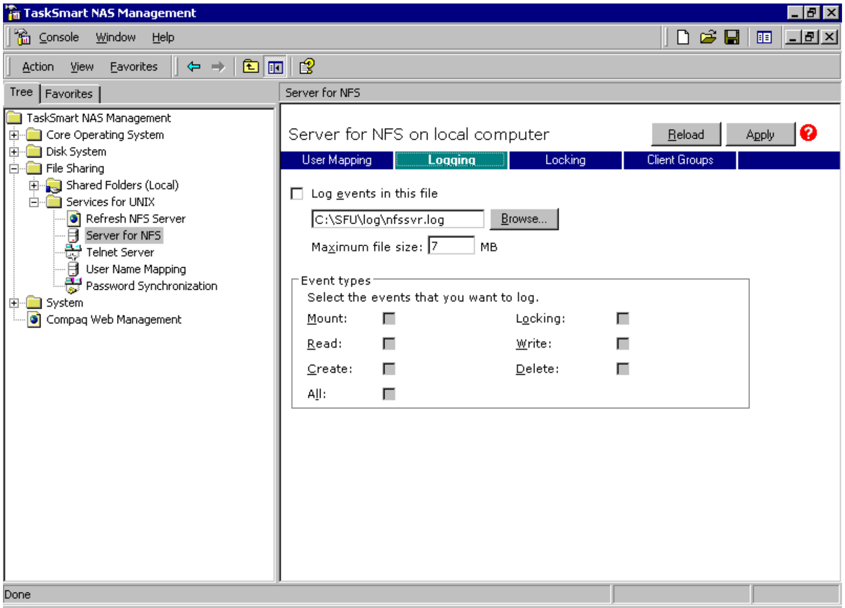
User mapping and authentication are performed by a computer running User Name Mapping. This service stores the mappings that associate Windows users or groups with UNIX users or groups. Specify the name of the computer that you want to use.

Computer name: localhost

Figure 4-2. Server for NFS on local computer, User Mapping scren

Logging Events

1. Select the **Logging** tab from the Server for NFS pane.
2. To log selected event types, click the check box for “Log events in this file” on the screen.
3. When logging, provide a filename or use the default filename provided (rootdrive\SFU\log\nfssvr.log) and log file size (7-MB default). The default log file is not initially created but is created when you apply the changes.



Server for NFS on local computer

☐ Log events in this file

C:\SFU\log\nfssvr.log

Maximum file size: 7 MB

Event types

Select the events that you want to log.

Mount: ☐ Locking: ☐

Read: ☐ Write: ☐

Create: ☐ Delete: ☐

All: ☐

Figure 4-3. Server for NFS on local computer, Logging pane

User Name Mapping

Another component of SFU is the User Name Mapping Server. This section defines and describes the purpose of user name mapping.

User name mapping is the process of taking user and group identification from one environment and translating it into user identification in another environment.

In the context of UNIX and NFS, user and group identification is a combination of a user ID (UID) and group ID (GID). In Windows environments, a user identification is a Security ID (SID) or Globally Unique Identifier (GUID) for Windows 2000.

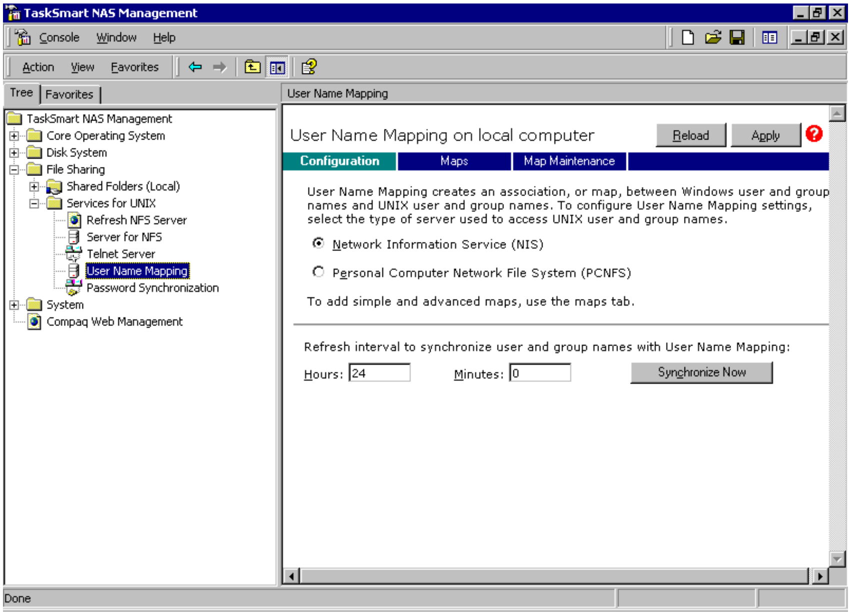
When a fileserver is exporting files within a homogeneous environment, there are no problems with authentication. It is a simple matter of making a direct comparison to determine whether the user should be allowed access to the file, and what level of access to allow.

However, when a fileserver is working in a heterogeneous environment, some method of translating user access is required. User mapping is the process of translating the user security rights from one environment to another.

As described in the previous section, the NFS server grants or denies access to the export based on machine name or IP address. However, once the client machine has access to the export, user-level permissions are used to grant or deny access to user files and directories.

The TaskSmart N2400 appliance is capable of operating in a heterogeneous environment, meaning that it is able to work with both UNIX and Windows clients. Because the files are stored in the native Windows NT file system, the server has to map the UNIX users to Windows users to determine the user access level of the files.

NOTE: User mapping is not designed to address existing user database problems in the existing environment. All UIDs and GIDs must be unique across all NIS (Network Information Service) domains and all user names must be unique across all Windows NT domains.



User Name Mapping on local computer

User Name Mapping creates an association, or map, between Windows user and group names and UNIX user and group names. To configure User Name Mapping settings, select the type of server used to access UNIX user and group names.

● Network Information Service (NIS)

○ Personal Computer Network File System (PCNFS)

To add simple and advanced maps, use the maps tab.

Refresh interval to synchronize user and group names with User Name Mapping:

Hours: 24 Minutes: 0

Figure 4-4. User Name Mapping user interface

Implementation

The user name mappings are most easily done in the SFU MMC. Although there is a command-line interface for the mapping server, the GUI interface makes it very easy to map users.

The mapping server makes a distinction between two different modes of operation:

- simple
- advanced

In simple mode, user and group names that match exactly in name across Windows and UNIX are automatically equated by user name. This matching is done automatically by the user name mapping server. The administrator can disable this feature.

> **NOTE:** If this feature is turned off, the administrator must use advanced mode and manually map all users.

In advanced mode, the administrator can manually map any users and groups to any other users and groups. Advanced maps override simple maps, giving administrators the capability of using simple mapping for most users and then using advanced mappings to make changes to simple mappings. This combination makes the job of the administrator much easier.

SFU currently supports squashing. The default user is ANONYMOUS LOGON, but this default user can be changed. For more details on how to change the default squashing user, see the Compaq "OEM Supplemental Help" chapter of the SFU help, found on the TaskSmart N2400 console.

Figure 4-5 is a diagram showing an example of how the mapping server works for an `ls -al` command.

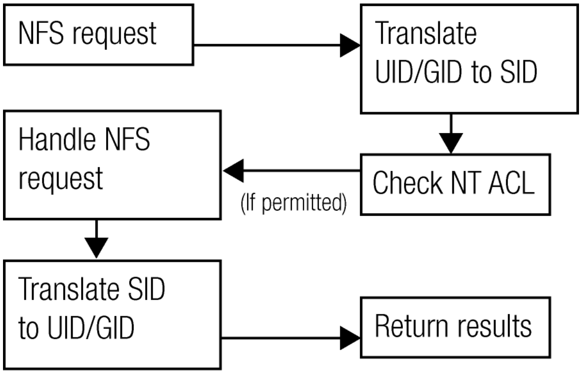


Figure 4-5. Mapping server "ls –al" command example

A double translation, as illustrated in Figure 4-5, is sometimes necessary because some commands return user ID information. For example, if the NFS request issued was an `ls -al` command, the return listing of files contains user information (the user and group that own the file). The `ls –al` command is a Unix command. It returns a long or full listing of all files. Because this information is contained in a Windows NT Access Control List (ACL), it is not UNIX ready. The ACL information has to be converted back to UNIX UIDs and GIDs for the UNIX systems to understand and display the user information.

This second translation is not done for commands that do not return user information. For example, if the NFS request were just to read data from or write data to a file, the second translation would not be performed because there is no returning user information.

Requirement

- The Server for NFS Authentication software must be installed on all PDCs (Primary Domain Controllers) and BDCs (backup domain controllers) that have Windows NT users mapped to UNIX users. See the "Mapping Procedures" section later in this chapter for details.

Limitation

- User name mapping is systemwide, as opposed to export by export. In SFU, the location that the user is mapped to applies to all file systems. Any changes to the default squashing user are also systemwide.

Mapping Procedures

The TaskSmart N2400 appliance stores the data in an NTFS file system. The user name mapping server must translate the UNIX users into Windows users, so that the appliance can determine user access rights to the data.

The administrator designates the source of mapping information for both CIFS and NFS client users as follows:

- UNIX: Local files or NIS
- CIFS: Local or Windows NT domain

Installation of Server for NFS on a Domain Controller

1. Locate the sfucustom.msi file located in the SFU directory of the TaskSmart N2400 appliance.
2. On the domain controller where the service is being installed, do the following:

   Use Windows Explorer:

   a. Open the shared directory containing sfucustom.msi.
   b. Double-click the file to open it. Windows Installer is opened.

   NOTE: If the domain controller used does not have Windows Installer installed, locate the file InstMSI.exe on the SFU directory and run it. After this installation, the Windows Installer program starts when opening sfucustom.msi

   c. Click **Next** when the Welcome to Windows Services for Unix screen is displayed.
   d. Enter the User name and Organization, and then click **Next.**
   e. Accept the license agreement, and then click **Next.**
   f. Select **Custom Installation,** and then click **Next.**
   g. Select the default to simply add Authentication Tools NFS for or add Will be installed on local hard drive option for Password Synchronization to have both installed on the DC.
   h. Select the installation directory, and then click **Next.**
   i. Click **Finish** when installation is complete.

   NOTE: Installing password synchronization requires a reboot of the server.

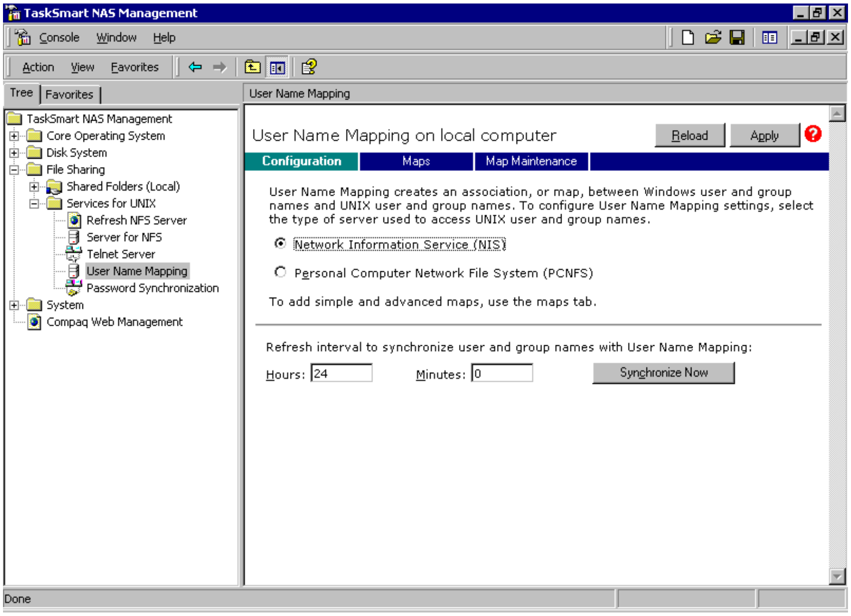
Simple User Maps

Two levels of mapping, simple and advanced, allow for user name matching. The administrator must determine the appropriate level of mapping.

Simple, or implicit, is the first level of user name mapping. Simple user name mapping automatically equates Windows NT logons and UNIX logons with matching spellings, whether they are actually the same users or not. The user name mapping service allows the administrator to disable implicit mapping.

The guidelines for simple user name mapping are as follows:

1. The administrator can map one or more Windows NT domains to one NIS domain.



User Name Mapping on local computer

User Name Mapping creates an association, or map, between Windows user and group names and UNIX user and group names. To configure User Name Mapping settings, select the type of server used to access UNIX user and group names.

● Network Information Service (NIS)

○ Personal Computer Network File System (PCNFS)

To add simple and advanced maps, use the maps tab.

Refresh interval to synchronize user and group names with User Name Mapping:

Hours: 24 Minutes: 0

Figure 4-6. NIS Configuration screen

2. For NIS configurations, the refresh field determines how often the mapping server connects to the NIS domains to update the UNIX user list. For PCNFS, the refresh field determines how often the files are refreshed from disk.

3. If the administrator is not using NIS, the following files from the UNIX machine must be obtained and copied to the TaskSmart N2400 appliance:

   -/etc/password

   -/etc/group

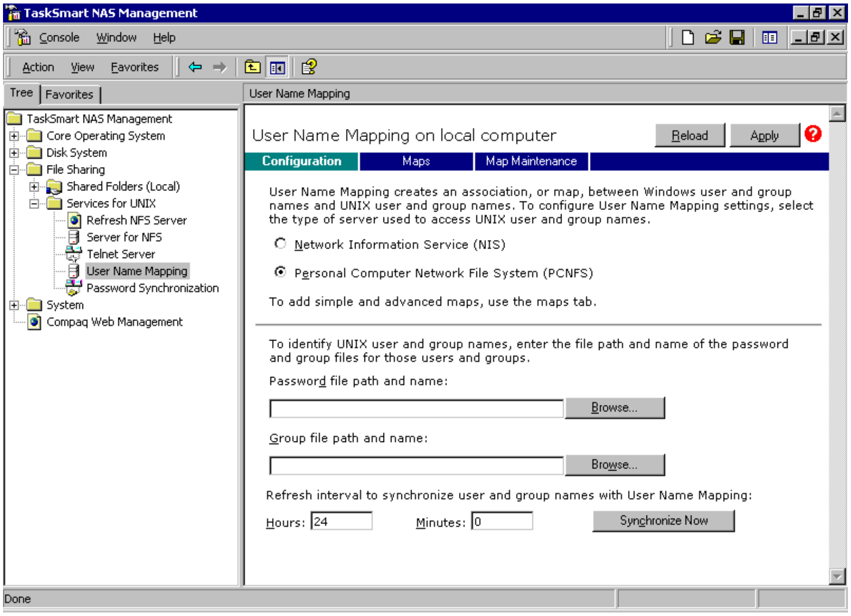
Creating and Viewing Simple User Maps Using PCNFS

1. Click the **User Name Mapping** control and select the **Configuration** tab.

   Figure 4-7 illustrates the PCNFS Configuration screen.

2. Click **Personal Computer Network File System (PCNFS)**.

3. After this option button is selected, the **Password** and **Group** are displayed. In both boxes, type the path and name of the local password and group files, or click **Browse** to locate the files.



User Name Mapping creates an association, or map, between Windows user and group names and UNIX user and group names. To configure User Name Mapping settings, select the type of server used to access UNIX user and group names.

○ Network Information Service (NIS)

● Personal Computer Network File System (PCNFS)

To add simple and advanced maps, use the maps tab.

To identify UNIX user and group names, enter the file path and name of the password and group files for those users and groups.

Password file path and name:

Group file path and name:

Refresh interval to synchronize user and group names with User Name Mapping:

Hours: 24 Minutes: 0

Figure 4-7. PCNFS configuration screen

4. Select the **Maps** tab.

5. Click the **Simple Maps** check box.

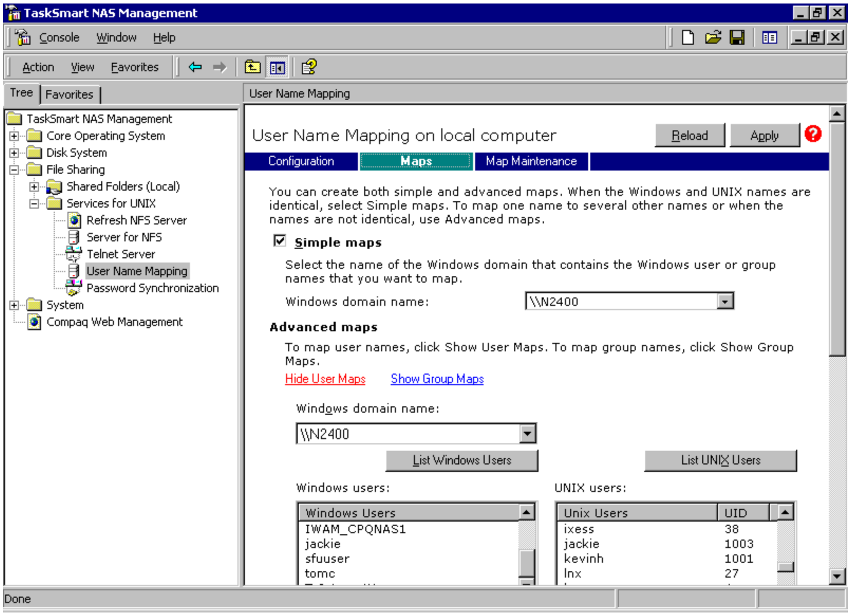
6. Select the Windows Domain name that you want to map.

IMPORTANT: Only one domain can have simple mappings. For information about how to set up simple maps for multiple domains, see the Compaq "OEM Supplemental Help" chapter of the SFU help, found on the TaskSmart N2400 console.

---

7. Click **Apply** at the top of the pane to save changes.
8. In the Advanced Maps section, click **Show Users Maps,** or **Show Groups Maps,** depending on what type of map that you want to list.

NOTE: When mapping multiple Windows domains, you can choose the Windows domain from the Windows domain name combo box. Multiple domains are listed only if domain trusts have been established.



User Name Mapping on local computer

You can create both simple and advanced maps. When the Windows and UNIX names are identical, select Simple maps. To map one name to several other names or when the names are not identical, use Advanced maps.

☑ Simple maps

Select the name of the Windows domain that contains the Windows user or group names that you want to map.

Windows domain name: \\N2400

Advanced maps

To map user names, click Show User Maps. To map group names, click Show Group Maps.

Windows domain name: \\N2400

Windows users:

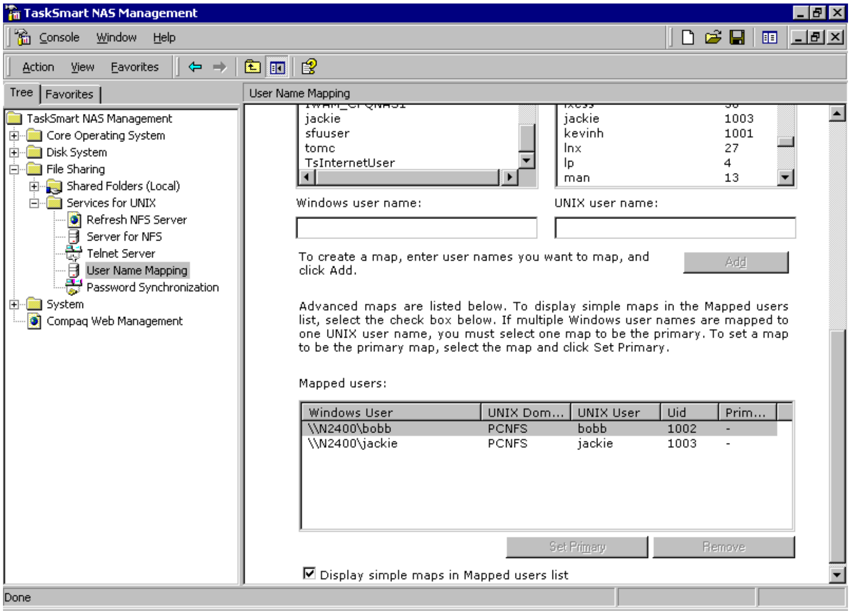
Windows Users
IWAM_CPQNAS1
jackie
sfuuser
tomc

UNIX users:

Unix Users	UID
ixess	38
jackie	1003
kevinh	1001
lnx	27

Figure 4-8. Simple maps for PCNFS - Show User Maps dialog box (top portion)

9. Check the **Display simple maps in Mapped users list** check box at the bottom of the screen. The screen lists the maps that match in spelling for Windows and UNIX.



jackie
sfuuser
tomc
TsInternetUser

jackie	1003
kevinh	1001
lnx	27
lp	4
man	13

Windows user name:

UNIX user name:

To create a map, enter user names you want to map, and click Add.

Advanced maps are listed below. To display simple maps in the Mapped users list, select the check box below. If multiple Windows user names are mapped to one UNIX user name, you must select one map to be the primary. To set a map to be the primary map, select the map and click Set Primary.

Mapped users:

Windows User	UNIX Dom...	UNIX User	Uid	Prim...
\\N2400\bobb	PCNFS	bobb	1002	-
\\N2400\jackie	PCNFS	jackie	1003	-

☑ Display simple maps in Mapped users list

Figure 4-9. Simple maps for PCNFS - Show User Maps dialog box (bottom portion)

NOTE: Figure 4-9 lists the simple user maps. To view the simple group maps, click **Show Group Maps**, and then select the **Display simple maps in Mapped Groups** check box. The maps are then displayed in the **Mapped groups** box.

Creating and Viewing Simple User Maps Using NIS

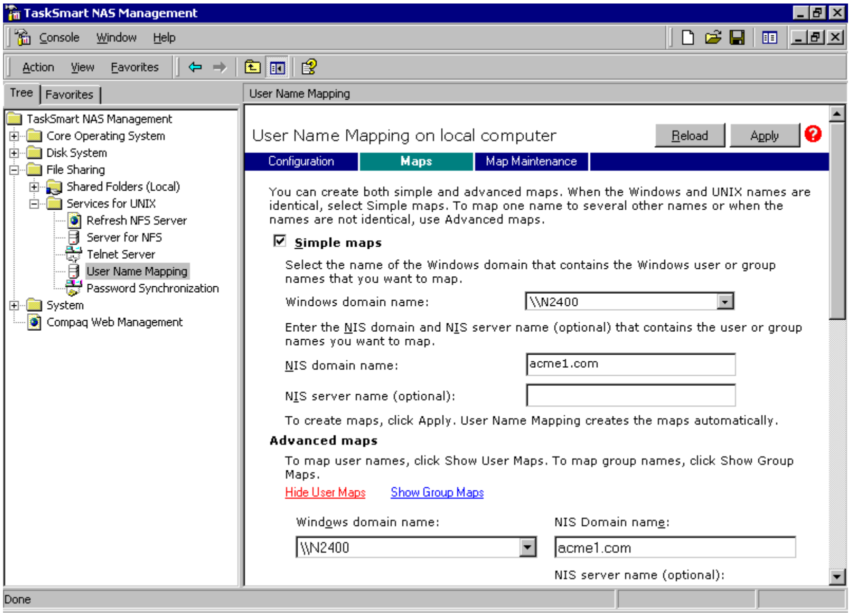
1. Click the **User Name Mapping** control and select the **Configuration** tab.
2. Click **Network Information Service (NIS)**.
3. Select the **Maps** tab.
4. Click the **Simple Maps** box.

5. Select the Windows Domain name that you want to map.

IMPORTANT: Only one domain can have simple mappings. For information about how to set up simple maps for multiple domains, see the Compaq “OEM Supplemental Help” chapter of the SFU help, found on the TaskSmart N2400 console.

---

6. Enter the domain name of the NIS server.
7. Enter the NIS server name. (optional)
8. Click **Apply** at the top of the pane to save changes.
9. In the Advanced Map section, click **Show Users Maps** or **Show Groups Maps,** depending on what type of map that you want to list.



User Name Mapping on local computer

You can create both simple and advanced maps. When the Windows and UNIX names are identical, select Simple maps. To map one name to several other names or when the names are not identical, use Advanced maps.

☑ **Simple maps**

Select the name of the Windows domain that contains the Windows user or group names that you want to map.

Windows domain name: \\N2400

Enter the NIS domain and NIS server name (optional) that contains the user or group names you want to map.

NIS domain name: acme1.com

NIS server name (optional):

To create maps, click Apply. User Name Mapping creates the maps automatically.

Advanced maps

To map user names, click Show User Maps. To map group names, click Show Group Maps.

Windows domain name: \\N2400

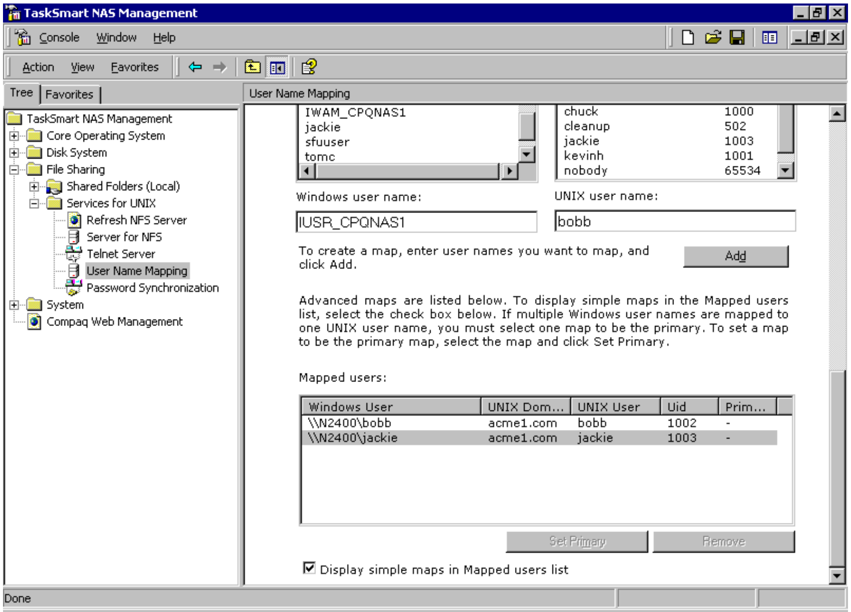
NIS Domain name: acme1.com

NIS server name (optional):

Figure 4-10. Simple maps for NIS - Show User Maps dialog box

NOTE: When mapping multiple Windows domains, you can choose the Windows domain from the Windows domain name combo box. Multiple domains are listed only if domain trusts have been established.

10. Click the **Display simple maps in Mapped users list** check box. The screen lists maps that match in spelling for Windows and UNIX NIS.



IWAM_CPQNAS1
jackie
sfuuser
tomc

chuck	1000
cleanup	502
jackie	1003
kevinh	1001
nobody	65534

Windows user name: IUSR_CPQNAS1

UNIX user name: bobb

To create a map, enter user names you want to map, and click Add.

Advanced maps are listed below. To display simple maps in the Mapped users list, select the check box below. If multiple Windows user names are mapped to one UNIX user name, you must select one map to be the primary. To set a map to be the primary map, select the map and click Set Primary.

Mapped users:

Windows User	UNIX Dom...	UNIX User	Uid	Prim...
\\N2400\bobb	acme1.com	bobb	1002	-
\\N2400\jackie	acme1.com	jackie	1003	-

☑ Display simple maps in Mapped users list

Figure 4-11. Simple maps in mapped users list for NIS dialog box

NOTE: Figure 4-11 lists the simple user maps. To look at the simple group maps, click **Show Group Maps**, and then select the **Display simple maps** check box in Mapped groups list. The maps are then displayed in the **Mapped groups** box.

Advanced User Maps

Advanced, or explicit, is the second level of user name mapping. Advanced user name mapping allows the administrator to specifically decide how matching is accomplished. The administrator manually lines up the Windows NT and UNIX user and group names.

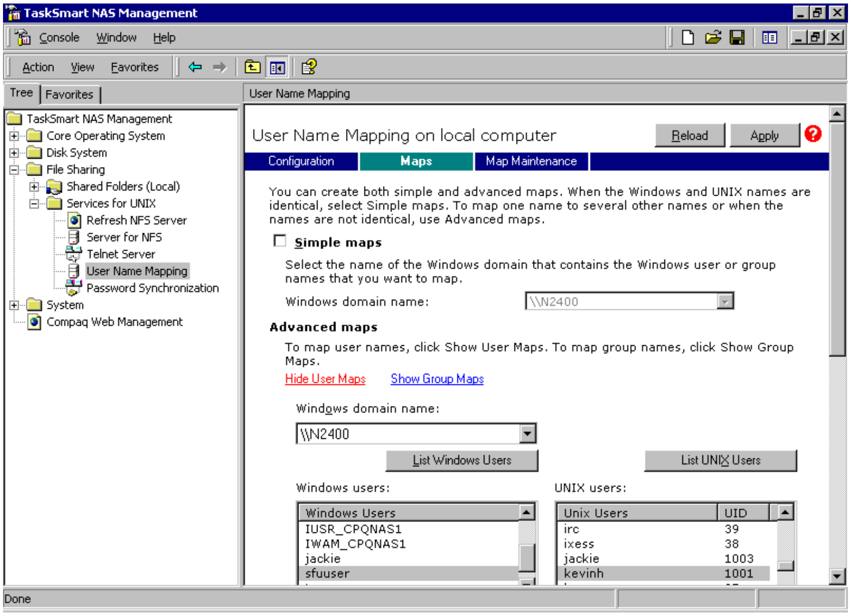
When mapping multiple Windows users to a single UNIX user, the administrator must map a primary user when using advanced mapping. The first mapping created is defaulted as the primary mapping. When additional mappings are created for the UNIX user, the administrator can change the primary map.

Creating Advanced Maps Using PCNFS

1. Click the **User Name Mapping** control, and then select the **Configuration** tab.

   Figure 4-7 illustrates the PCNFS Configuration screen.

2. Select the **Personal Computer Network File System (PCNFS)** option button.
3. After this option button is selected, the **Password** and **Group** are displayed. In both boxes, type the path and name of the local password and group files, or click **Browse** to locate the files. See “Creating and Viewing Simple User Maps Using PCNFS” earlier in this chapter for details on password and group files.
4. Click the **Maps** tab.



User Name Mapping on local computer

You can create both simple and advanced maps. When the Windows and UNIX names are identical, select Simple maps. To map one name to several other names or when the names are not identical, use Advanced maps.

☐ **Simple maps**

Select the name of the Windows domain that contains the Windows user or group names that you want to map.

Windows domain name: \\N2400

Advanced maps

To map user names, click Show User Maps. To map group names, click Show Group Maps.

Windows domain name: \\N2400

Windows users:

Windows Users
IUSR_CPQNAS1
IWAM_CPQNAS1
jackie
sfuuser

UNIX users:

Unix Users	UID
irc	39
ixess	38
jackie	1003
kevinh	1001

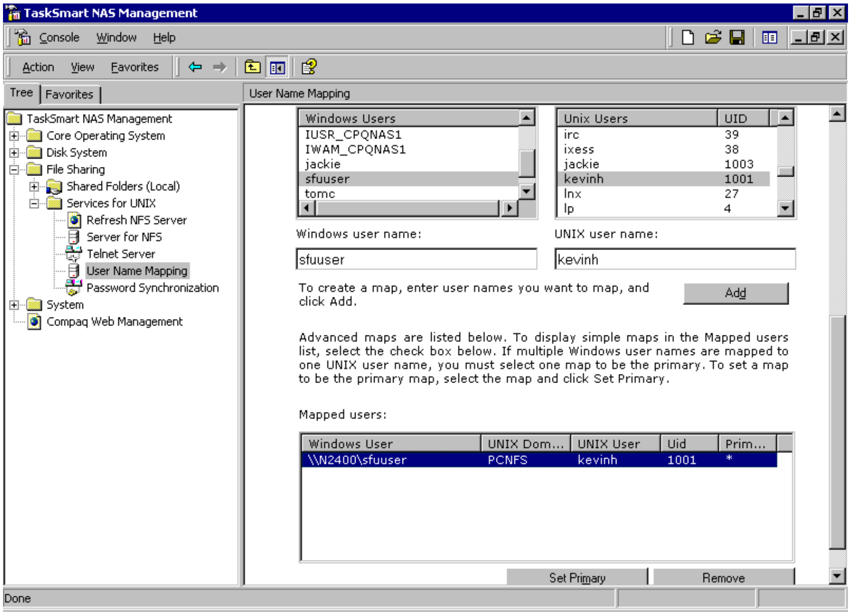
Figure 4-12. Advanced maps for PCNFS - Show User Maps dialog box

5. Click **List Windows Users** to see the Windows users.

   NOTE: When mapping multiple Windows domains, you can choose the Windows domain from the Windows domain name combo box. Multiple domains are only listed if domain trusts have been established.

6. Click the **List UNIX Users** button to see the UNIX users that are displayed in the password file supplied in the Configuration section.

7. Highlight the **Windows user** and **UNIX user** that you want to map, and then click **Add.**



Windows Users
IUSR_CPQNAS1
IWAM_CPQNAS1
jackie
sfuuser
tomc

Unix Users	UID
irc	39
ixess	38
jackie	1003
kevinh	1001
lnx	27
lp	4

Windows user name: sfuuser

UNIX user name: kevinh

To create a map, enter user names you want to map, and click Add.

Advanced maps are listed below. To display simple maps in the Mapped users list, select the check box below. If multiple Windows user names are mapped to one UNIX user name, you must select one map to be the primary. To set a map to be the primary map, select the map and click Set Primary.

Mapped users:

Windows User	UNIX Dom...	UNIX User	Uid	Prim...
\\N2400\sfuuser	PCNFS	kevinh	1001	*

Figure 4-13. Windows user and UNIX user to map and add for PCNFS dialog box

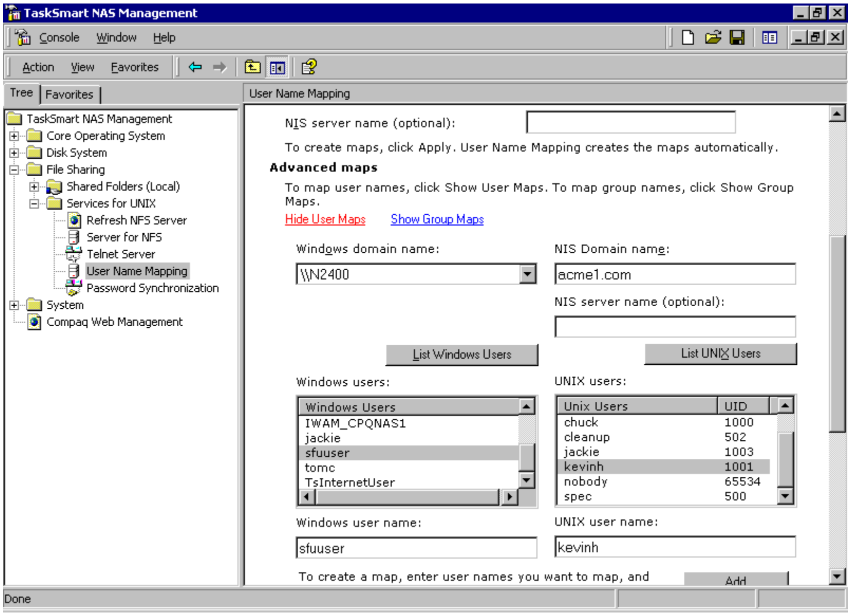
8. Repeat step 7 until you have mapped all the desired users.

9. Click **Apply** at the top of the pane to save changes.

NOTE: The procedures for creating user and group mappings are the same. The UNIX group names are displayed in the Configuration section of the screen. The list of Windows and UNIX groups can be displayed by clicking **Show Group Maps** found in the Advanced maps section of the screen and listing the Windows and UNIX groups as shown in the preceding steps.

Creating Advanced User Maps Using NIS

1. Select the **User Name Mapping** control.
2. Click the **Configuration** tab.
3. Select the **Network Information Service (NIS)** option button.
4. Click the **Maps** tab.
5. Click **Show Users** or **Show Groups,** depending on what type of map that you want to create. This link is displayed in the Advanced maps section.



NIS server name (optional):

To create maps, click Apply. User Name Mapping creates the maps automatically.

Advanced maps

To map user names, click Show User Maps. To map group names, click Show Group Maps.

Windows domain name: \\N2400

NIS Domain name: acme1.com

NIS server name (optional):

Windows users:

Windows Users
IWAM_CPQNAS1
jackie
sfuuser
tomc
TsInternetUser

UNIX users:

Unix Users	UID
chuck	1000
cleanup	502
jackie	1003
kevinh	1001
nobody	65534
spec	500

Windows user name: sfuuser

UNIX user name: kevinh

To create a map, enter user names you want to map, and

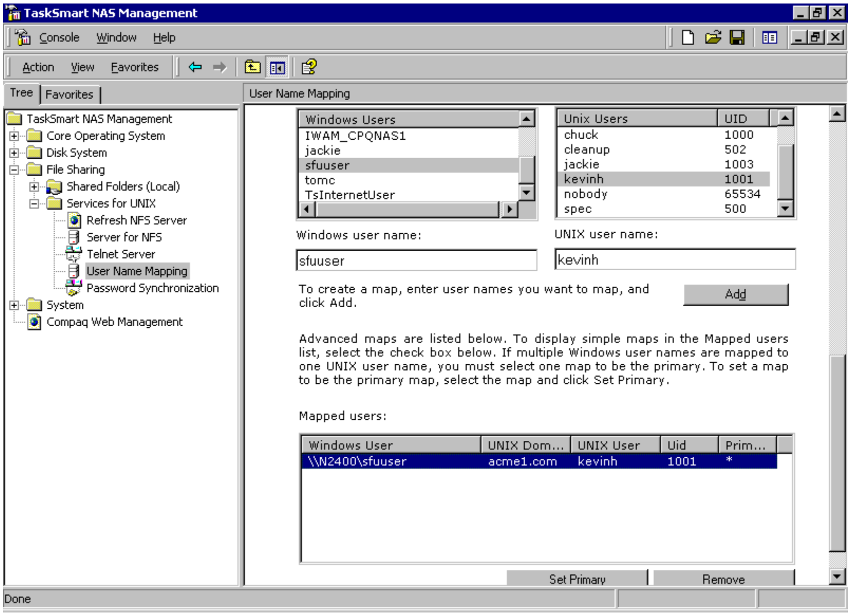
Figure 4-14. Advanced maps for NIS, Show User Maps dialog box

6. Click **List Windows Users** to show the Windows users.

NOTE: When mapping multiple Windows domains, you can choose the Windows domain from the Windows domain name combo box. Multiple domains are listed only if domain trusts have been established.

7. Type the NIS domain name in the NIS Domain name box. NIS server name is optional.
8. Click **List UNIX Users** to show the UNIX users in the NIS domain.

9. Highlight the **Windows user** and **UNIX user** that you want to map, and then click **Add**.



Windows Users
IWAM_CPQNAS1
jackie
sfuuser
tomc
TsInternetUser

Unix Users	UID
chuck	1000
cleanup	502
jackie	1003
kevinh	1001
nobody	65534
spec	500

Windows user name: sfuuser

UNIX user name: kevinh

To create a map, enter user names you want to map, and click Add.

Advanced maps are listed below. To display simple maps in the Mapped users list, select the check box below. If multiple Windows user names are mapped to one UNIX user name, you must select one map to be the primary. To set a map to be the primary map, select the map and click Set Primary.

Mapped users:

Windows User	UNIX Dom...	UNIX User	Uid	Prim...
\\N2400\sfuuser	acme1.com	kevinh	1001	*

Figure 4-15. Windows users and UNIX users to map and add for NIS dialog box

10. Repeat step 10 until you have mapped all of the users.

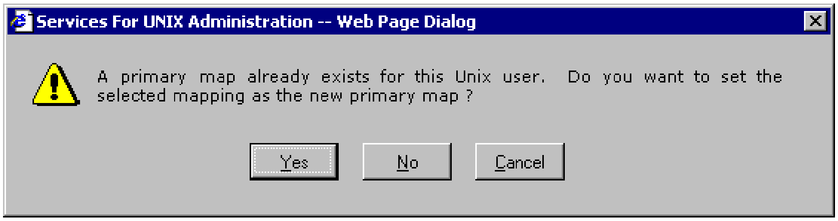
11. Click **Apply** at the top of the pane to save changes.

NOTE: The procedures for creating user and group mappings are identical. The list of Windows and UNIX groups is displayed by clicking Show Group Maps in the Advanced maps section of the screen and by displaying the Windows and UNIX groups as shown in the preceding steps.

Primary Mapping

When an initial mapping is created for a user or group, it is marked as primary by default. If you attempt to create multiple maps for one Unix user or group to multiple Windows users or groups, then you will be asked to choose which mapping to set primary.

1. Highlight the map that you want to assign as primary.
2. Click the **Set Primary** button. The dialog box illustrated in Figure 4-16 is displayed.



A primary map already exists for this Unix user. Do you want to set the selected mapping as the new primary map ?

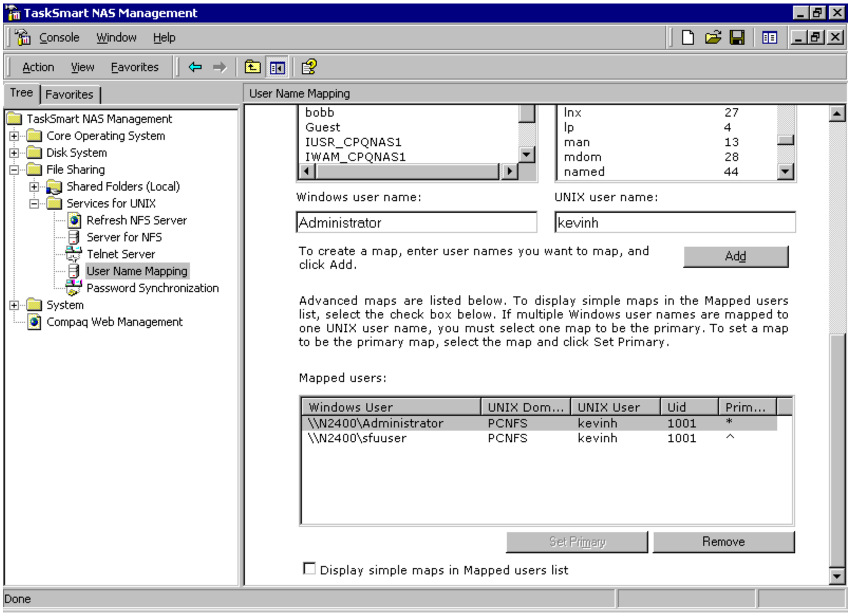
Figure 4-16. Set primary user mapping

3. Click **Yes** to have the new mapping selected as primary.
4. Click **Apply** at the top of the pane to save changes.

NOTE: An asterisk listed in the Mapped users or groups section denotes that the mapping is primary.

Changing Primary Mapping

If you attempt to create multiple maps for one Unix user or group to multiple Windows users or groups, then you will be asked to choose which mapping to set primary.



Windows user name: Administrator

UNIX user name: kevinh

To create a map, enter user names you want to map, and click Add.

Advanced maps are listed below. To display simple maps in the Mapped users list, select the check box below. If multiple Windows user names are mapped to one UNIX user name, you must select one map to be the primary. To set a map to be the primary map, select the map and click Set Primary.

Mapped users:

Windows User	UNIX Dom...	UNIX User	Uid	Prim...
\\N2400\Administrator	PCNFS	kevinh	1001	*
\\N2400\sfuuser	PCNFS	kevinh	1001	^

☐ Display simple maps in Mapped users list

Figure 4-17. Primary User Mapping applied

To change the primary user mapping, perform the following steps:

1. Highlight the map that you want to assign as primary.
2. Click **Set Primary**.
3. Click **Yes** to have the new mapping selected as primary
4. Click **Apply** at the top of the pane to save changes.

NOTE: These same procedures are used to create or change primary group mappings.

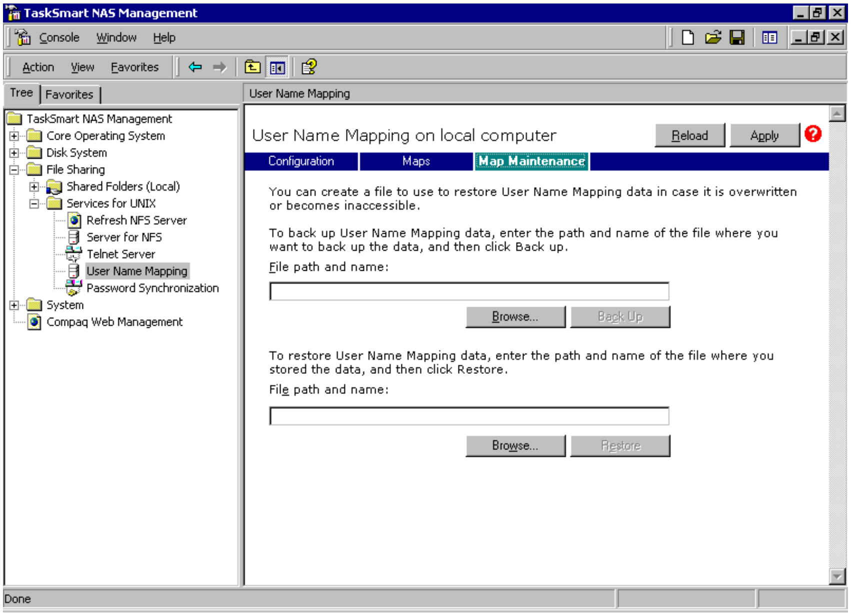
Multiple Domains and Multiple NIS Support

SFU supports simple and advanced user mappings between one or more Windows NT domains and one or more NIS domains. The default SFU setup supports multiple Windows NT domains to a single NIS domain. For information about setting up SFU to map users in multiple NIS domains, please consult the Compaq Supplemental Help section in the SFU online help for more information on setting up simple maps among multiple Windows NT and NIS domains.

Backup and Restoration of Mappings

The user name mapping server has the capability to save and retrieve mappings from files. This capability is useful for backing up mapping settings prior to making changes and for exporting the mapping file from one server to others, using the same mapping information.

The user name mapping server can save existing mappings to a file or load them from a file and populate the mapping server. This feature is found under the Map Maintenance tab of the User Name Mapping display window, as shown in Figure 4-18.



You can create a file to use to restore User Name Mapping data in case it is overwritten or becomes inaccessible.

To back up User Name Mapping data, enter the path and name of the file where you want to back up the data, and then click Back Up.

File path and name:

To restore User Name Mapping data, enter the path and name of the file where you stored the data, and then click Restore.

File path and name:

Figure 4-18. Map Maintenance

Backup Mapping Procedure

1. Select the **Map Maintenance** tab from the User Name Mapping control.
2. Type the path and name of the file to be used for backup in the **File path and name** field, or click **Browse** to locate the file.

   NOTE: If you are creating the file for the first time, follow these steps:

   1. Browse to the target directory.
   2. Right-click in the file listing pane, select New, Text Document. Enter a name for the file, and then press the **Enter** key on your keyboard.
   3. Double-click the new file to select it.

3. Click **Backup.**

Restore Mapping Procedure

1. Select the **Map Maintenance** tab from the User Name Mapping control.
2. Type the path and name of the file in the **File path and name** field, or click **Browse** to locate the file.

   NOTE: If you are creating the file for the first time, follow these steps:

   1. Browse to the target directory.
   2. Right-click in the file listing pane, select New, Text Document. Enter a name for the file, and then press the **Enter** key on your keyboard.
   3. Double-click the new file to select it.

3. Click **Restore.**

This feature is particularly useful when you back up user mappings to address server failures. You can implement redundant mapping servers for fault tolerance by pointing the NFS server to a mapping service on another TaskSmart N2400 appliance. For this feature to work properly, all the user name mappings must be the same.

NOTE: If mapping services are deployed in different departments, the user name mappings may be different.

Mortice Kern Systems Toolkit

The Mortice Kern Systems (MKS) Toolkit is a collection of UNIX utilities ported to the Windows NT 32-bit command console. Details about how to install and run these utilities are available in the online help documentation.

NFS File Exporting Using SFU

NFS is the exporting protocol for UNIX and Linux clients. NFS export permissions are independent of the CIFS share permissions. A particular directory, or drive, can be exported to:

- CIFS only
- NFS only
- CIFS and NFS

NFS export permissions are slightly different from Windows NT sharing. NFS exporting may specify read only or read/write permissions, and may specify one or more client system names that are granted access to the export. Exports with All Machines specified are open to all client systems.

Procedure for NFS Exporting

This section contains the basic procedure for NFS exporting. See the Microsoft Services for UNIX help files for more details on NFS exporting.

1. Double-click the **My Computer** icon on the desktop.
2. Create a new folder or select an existing folder in the Explorer interface.
3. Highlight the selected folder or virtual disk.
4. Right-click the item, and select **Sharing.** Then click the **NFS Sharing** tab.
5. Click the **Share this folder** option button, and then set the sharing name.
6. Click **Permissions** to set the export (or share) permissions, client groups, and root access, if desired.

Testing NFS

1. Be sure to establish a folder to export, and export it to NFS clients.
2. From a UNIX or Linux client, type:

   ```
   showmount -e TaskSmart N2400 name
   ```

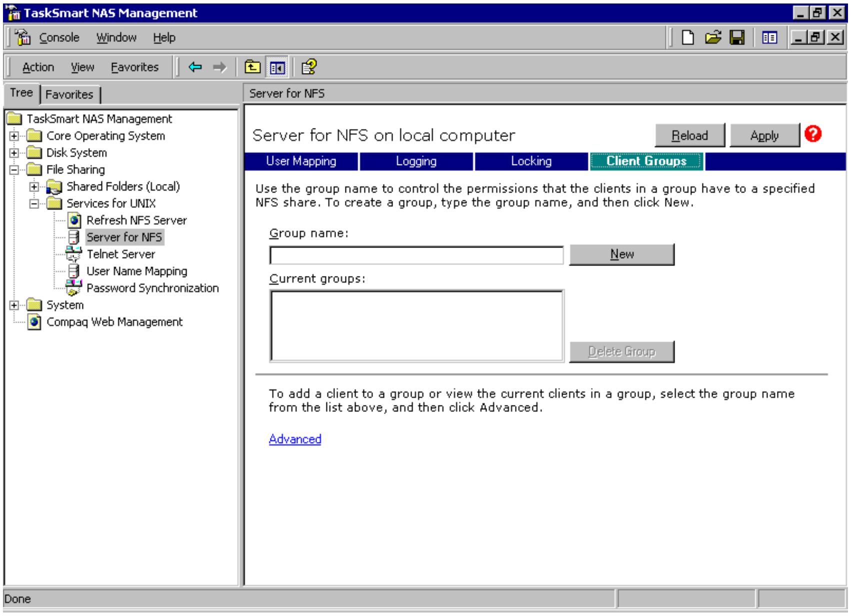
   NOTE: The showmount command works only after the TaskSmart N2400 name is added to the /etc/hosts file of the UNIX client, or if the DNS recognizes the TaskSmart N2400 name.

3. Compile a list of exported file systems that the TaskSmart N2400 appliance is exporting to NFS clients.
4. To associate an exported file system to the client directory called `/mount-point`, open the client console screen, and then type:

   ```
   mount –t nfs servername:/exportname /mount-point
   ```

Client Groups

The client groups feature gives administrators a method of assigning access permissions to a set of clients. The administrator creates a client group, gives it a name, and then inserts clients into the group by client name or IP address. After the client group is created, the administrator adds or removes permissions for the entire group, instead of allowing or denying access for each individual client machine.



Use the group name to control the permissions that the clients in a group have to a specified NFS share. To create a group, type the group name, and then click New.

To add a client to a group or view the current clients in a group, select the group name from the list above, and then click Advanced.

Figure 4-19. Client groups

NOTE: Currently, the client group is allowed to assume the same name as a client. When this duplication occurs, the client is obscured from the view of the server. For example, assume that a client d4 exists. If you create a client group called d4, you can no longer assign permissions to just the client d4. Any reference to d4 now refers to client group d4.

File Locking

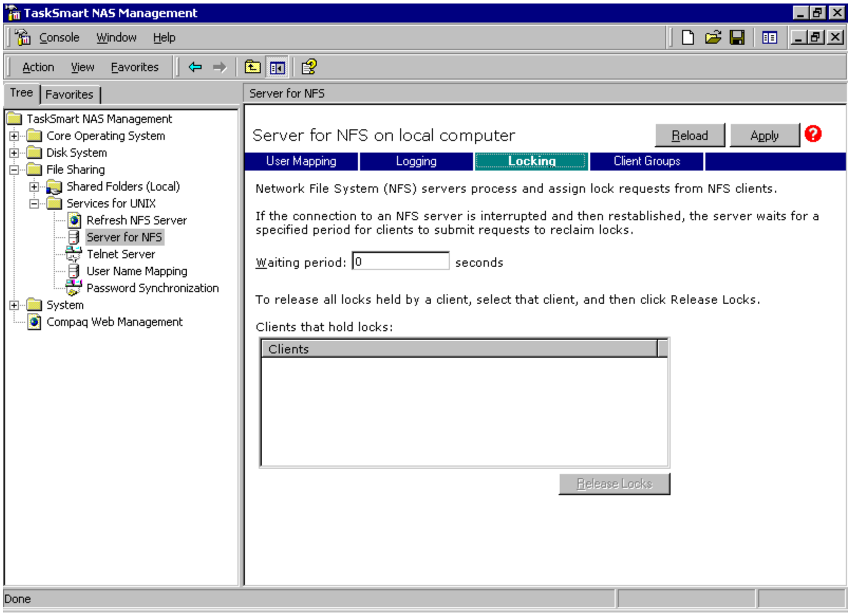
NFS supports the ability to lock files. File locking helps prevent two or more users from working with the same files at the same time.

For example, Microsoft Office or Star Office places a lock on an open file to prevent other users from editing the file at the same time. NFS has support for this action.

However, NFS locking is optional, but advisable. It is not forced on the user. NFS locking depends on the software application components to manage the locks. If an application does not lock a file, or if a second application does not check for locks before writing to the file, nothing prevents the users from overwriting files.

The waiting period setting determines how long the TaskSmart N2400 appliance allows the locks to be kept active after a client or server crash. The TaskSmart N2400 appliance keeps the locks active for the specified number of seconds, while querying the client to see if it wants to keep the lock. If the client responds within this time frame, the lock is kept active. Otherwise, the TaskSmart clears the lock.

The locking user interface also allows the administrator to manually clear locks. Figure 4-20 illustrates the SFU for NFS File Locking interface.



Network File System (NFS) servers process and assign lock requests from NFS clients.

If the connection to an NFS server is interrupted and then restablished, the server waits for a specified period for clients to submit requests to reclaim locks.

Waiting period: 0 seconds

To release all locks held by a client, select that client, and then click Release Locks.

Clients that hold locks:

Figure 4-20. SFU for NFS file locking

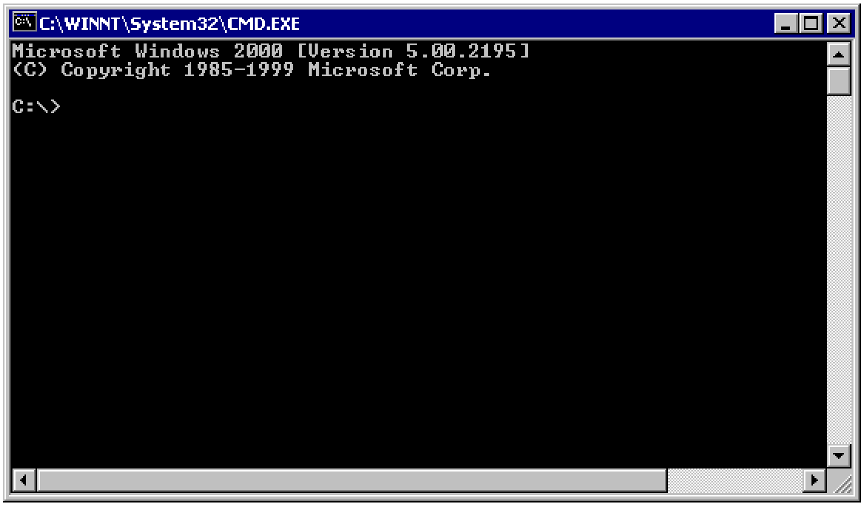
Auditing

Various levels of auditing are available. Auditing sends SFU events to a file for later review and establishes log-setting behavior. Some behavior examples include events logged and log file size. See the online SFU help for more information.

Command Line Capabilities

The command line provides the administrator flexibility to automate setups and other tasks through scripting. All of the SFU file-exporting tasks and other SFU activities can be accomplished from a command prompt.

Figure 4-21 and Table 4-1 illustrate and describe the command line interface.



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>
```

Figure 4-21. Command line interface

Table 4-1
Command Line Interface Command Prompts

Command	Function
nfsstat /?	Learn about viewing statistics by NFS operation type
showmount /?	View the format of the command to display NFS export settings on NFS servers
showmount -a	View users who are connected and what they currently have mounted
showmount -e	View exports from the server and their export permissions
rpcinfo /?	Learn how to display Remote Procedure Call (RPC) settings and statistics.
mapadmin /?	View how to add, delete, or change user name mappings
tnadmin /?	View how to change Telnet Server settings
nfsshare /?	Learn how to display, add, and remove exported shares

Chapter 5

Remote Administration

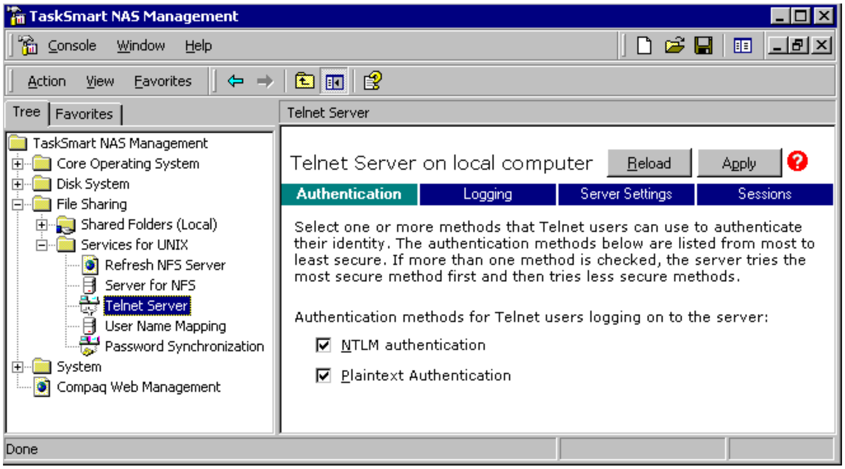
Remote Administration

The Compaq TaskSmart N2400 appliance is capable of remote administration by each of the following five methods:

- Telnet Server
- Remote Shell Daemon
- Remote Insight Lights-Out Edition board
- Web User Interface
- *Compaq Insight Manager*™ software
- Enterprise Management Applications
    - ❑ HP OpenView
    - ❑ Compaq Insight Manager for HP OpenView, Version 2.0
    - ❑ Tivoli NetView (AIX)
    - ❑ Compaq Insight Manager for Tivoli NetView (AIX), Version 2.0

Telnet Server

Telnet Server is a UNIX command line utility that allows users to connect to machines, log on, and obtain a command prompt remotely. To allow users Telnet Server access, the Telnet Server software must be installed. Telnet Server is preinstalled on the TaskSmart N2400 appliance.



Select one or more methods that Telnet users can use to authenticate their identity. The authentication methods below are listed from most to least secure. If more than one method is checked, the server tries the most secure method first and then tries less secure methods.

Authentication methods for Telnet users logging on to the server:

☑ NTLM authentication

☑ Plaintext Authentication

Figure 5-1. Telnet Server interface screen

The utility enables remote administration and user access from other machines.

Authentication

Use the authentication page to select user authentication methods allowed by the Telnet Server. The administrator determines what method of authentication is appropriate based on work environment.

Auditing

Telnet Server can log various events. The auditing page allows the administrator to enable logging and select the events that should be logged. Note that errors and significant events are always logged to the Windows 2000 event log as well.

Server Settings

Use the Telnet Server settings page to change Telnet Server parameters. These parameters determine how the TaskSmart N2400 Telnet Server operates. For example, one parameter is the number of simultaneous Telnet Server connections that the server allows.

Sessions

The sessions screen provides the ability to view or terminate active sessions.

Remote Shell Daemon

The remote shell, commonly referred to as "rsh" in UNIX, is a method for allowing users to access a command prompt or to run a command on another machine. It can be used in a fashion similar to Telnet Server or can be used to directly invoke a remote command.

For example:

```
rsh <server name> ls -al
```

The remote shell runs the `ls -al` command on <server name> and returns the results to your screen.

NOTE: A *.RHOSTS* file must be created to allow client access to the server. See the SFU help topic “Rshsvc” on how to create the *.RHOSTS* file.

Currently, SFU implements only the remote command functionality of rsh. If the users need a command line, they can use Telnet Server.

For more information regarding the setup and use of remote shell or the remote shell service, refer to the online help documentation.

Remote Insight Lights-Out Edition Board

The following information provides an overview of the Remote Insight Lights-Out Edition board capabilities. Refer to the *Compaq Remote Insight Lights-Out Edition Installation and Users Guide* on the Documentation CD for further information.

The Remote Insight Lights-Out Edition board is a PCI-based, single-board computer that uses a Web interface to provide remote management for the server from a remote console. Complete keyboard, mouse, and video capability for the server is available, regardless of the state of the host operating system or the host CPU. A built-in processor, combined with a standard external power supply, makes the Remote Insight Lights-Out Edition board independent of the host server and its operating system. The Remote Insight Lights-Out Edition board provides remote access, sends alerts, and performs other management functions, even if the host server operating system is not responding or the server has lost power.

The Remote Insight Lights-Out Edition board provides the following features:

- Hardware-based graphical remote console access

  IMPORTANT: The remote client console must have a direct browser connection to the Remote Insight Lights-Out Edition board without passing through a proxy server or firewall.

- Remote restart
- Server failure alerting
- Integration with Compaq Insight Manager
- Local Area Network (LAN) access through onboard NIC
- Browser support for Internet Explorer 4.01 or later
- Reset and failure sequence replay
- Remote Insight Lights-Out Edition User Administration Security
- External power
- Auto configuration of IP address via domain name system (DNS) or Dynamic Host Configuration Protocol (DHCP)
- Virtual power button

- Manage Users feature—allows the user with supervisory access to add or delete users, or modify an existing user’s configuration. Manage Users also allows the user to modify the following:
    - User name
    - Logon name
    - Password/confirm password
    - Simple network management protocol (SNMP) trap IP address
    - Receive host OS-generated SNMP traps
    - Supervisor access
    - Logon access
    - Remote console access
    - Remote server reset access
- Manage Alerts feature—allows the user to send test alerts, to clear pending alerts, and to specify which type of alert messages to receive.
    - Select alert types received
    - Generate a global test alert
    - Generate an individual test alert
    - Clear pending alerts
    - Enable alerts

Refer to the Remote Insight Lights-Out Edition board user guide for more information about the Remote Insight Lights-Out Edition board features and functionality.

Remote Insight Lights-Out Edition Board Configuration

By default, the TaskSmart N2400 appliance comes from the factory with full remote manageability. The Remote Insight Lights-Out Edition board on the TaskSmart N2400 appliance is initially configured through the Offline Configuration Utility (OCU). SNMP is already enabled, the Compaq Insight Management Agents are preinstalled, and the Remote Insight Lights-Out Edition board is fully functional.

The Remote Insight Lights-Out Edition board comes with factory default settings, which the administrator can change. Administrators may want to add users, change SNMP trap destinations, or change networking settings. Refer to the *Remote Insight Lights-Out Edition Installation and Users Guide* for more information about changing these settings.

There are several methods for performing Remote Insight Lights-Out Edition board configuration changes:

- Initial Remote Insight Lights-Out Edition board access using the default DNS name

  The Remote Insight Lights-Out Edition board is preconfigured by the Offline Configuration Utility (OCU) CD with a default user name, password, DNS name, and IP address. These are:

  - USERNAME: Administrator
  - PASSWORD: (last four digits of the serial number)
  - DNS NAME: RIBXXXXXXXXXXXX (The 12 Xs are the MAC address of the Remote Insight Lights-Out Edition board.)
  - IP ADDRESS:
- Web interface
- Pressing **F8** for the Remote Insight Lights-Out Edition board configuration utility during a system restart

- Accessing the system utilities by pressing **F10** during a system restart
    a. Select System Configuration.
    b. Select Configure Hardware.
    c. Select Review or Modify Hardware Settings.
    d. Select View or Edit Details.
    e. Select Remote Insight Lights-Out Edition board.
    f. Change DNS name, network settings or users.
    g. Press F10 to save changes before exiting.
- Remote Insight Lights-Out Edition board—board configuration service
    - ❑ The Compaq TaskSmart N2400 appliance comes equipped with a Remote Insight Lights-Out Edition board configuration service. The service is a Windows 2000 service supplied by Compaq. It configures the network setting for the Remote Insight Lights-Out Edition board.
    - ❑ Initially the Remote Insight Lights-Out Edition board is preconfigured by the OCU. The Remote Insight Lights-Out Edition board configuration service is designed to periodically locate the offline configuration diskette.
    - ❑ The Remote Insight Lights-Out Edition board configuration service locates the diskette. The service then checks for the existence of a *CQNASRIB.CFG* file. This file is originally created by the OCU.
    - ❑ The service uses the read-only attribute of the configuration file to determine if the configuration should be applied.
    - ❑ On each poll cycle the service checks the read-only attribute of the configuration file. The poll interval ranges between 1 and 5 minutes. If the poll range is not set, the service configures the Remote Insight Lights-Out Edition board and sets a read-only attribute on the configuration file.
    - ❑ To re-enable the offline configuration diskette for Remote Insight Lights-Out Edition board configuration, the read-only attribute of the *CQNASRIB.CFG* file must be reset.
    - ❑ For the configuration to occur, the read-only attribute requires that the offline configuration diskette not be write protected.
    - ❑ It is recommended that the OCU be used to enable the offline configuration diskette. The Remote Insight Lights-Out Edition board uses the OCU before changing the read-only attribute on the *CQNASRIB* file.

Remote Access

Using the Web interface of a client machine is the recommended procedure for remotely accessing a server.

1. Type the actual Internet Protocol (IP) address of the Remote Insight Lights-Out Edition board into the URL field on a client browser program, such as Internet Explorer.
2. Supply user name and password for administrator.

Web User Interface

The TaskSmart N2400 appliance includes a Web-based user interface for the administrator to remotely manage the machine. The Web-based user interface provides user and group management, share management, SANworks Virtual Replicator (SWVR) management, and a subset of MicrosoftWindows 2000 operations. In addition, the Web-based user interface includes wizards to guide the administrator while performing repetitive tasks, for example, creating a share. To access the Web-based user interface, launch a Web browser and enter http://<*your TaskSmart machine name or IP address*>:3201/ in the address field. Online help for the Web interface is available.

Compaq Insight Manager

The TaskSmart N2400 appliance is equipped with the latest Compaq Insight Management Agents for Servers, allowing easy manageability of the server through Compaq Insight Manager, HP OpenView, and Tivoli NetView.

Compaq Insight Manager Version 4.70 or higher is needed to successfully manage the TaskSmart N2400 appliance. Compaq Insight Manager is a comprehensive management tool that monitors and controls the operation of Compaq servers and clients. Compaq Insight Manager consists of two components:

- Windows-based console application
- Server- or client-based management data collection agents

Management agents monitor over 1,000 management parameters. Key subsystems are instrumented to make health, configuration, and performance data available to the agent software. The agents act upon that data by initiating alarms in the event of faults. The agents also provide updated management information, such as network interface or storage subsystem performance statistics.

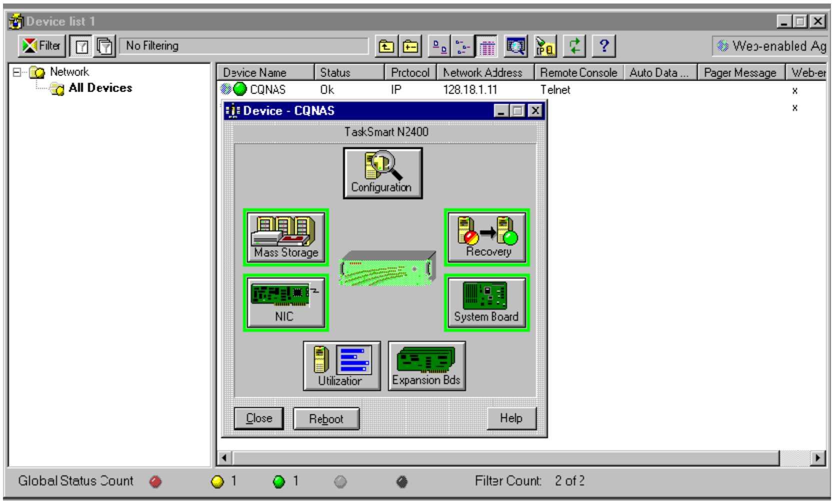
NOTE: The TaskSmart N2400 appliance also supports Compaq Insight Manager XE.

Compaq Insight Manager Console

System monitoring applications such as Compaq Insight Manager allow the administrator to accomplish normal administrative tasks from any remote location with a Web browser. To manage the TaskSmart N2400 appliance using the Compaq Insight Manager console:

1. Access the Discover IP devices from the Setup menu.
2. Click **New.**
3. Enter the IP address range of the device.
4. Click **Add.**
5. Click **Close** when finished.
6. Click **Find Devices.**
7. Select the device that you want to view.
8. Click **Add/Update All Devices.**
9. Double-click the server to show a device information window. The window allows the user to view management data collected by the Compaq agents.

Figure 5-2 is an example of the device information window.



Device Name	Status	Protocol	Network Address	Remote Console	Auto Data ...	Pager Message	Web-er
CQNAS	Ok	IP	128.18.1.11	Telnet			x
							x

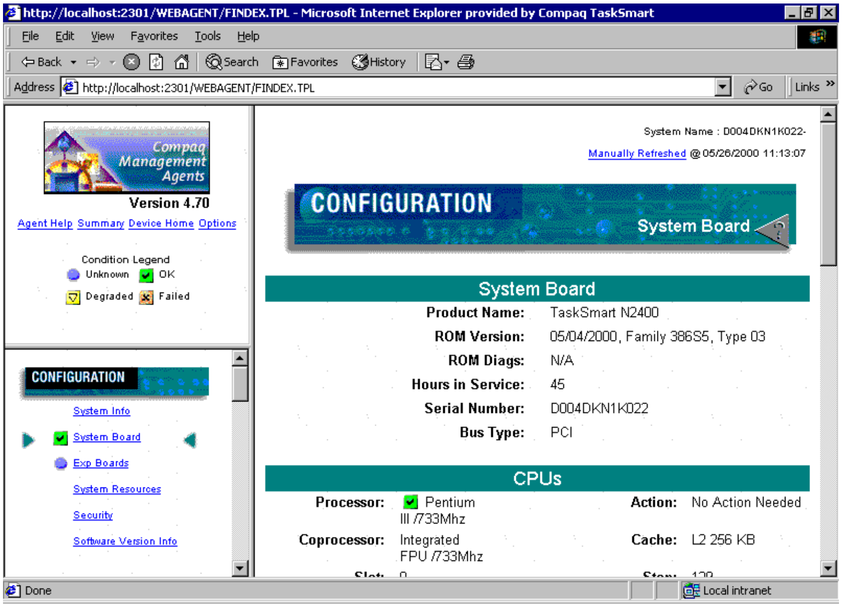
Figure 5-2. Device information window

For more information about using Compaq Insight Manager, see the Compaq Management CD.

Compaq Insight Manager Agent Web Interface

There are two options for accessing the Compaq Insight Manager Agent Web interface.

- From the Compaq Insight Manager console, right-click the device name and select **View Web Data.** The agent Web interface of the server launches in a browser within Compaq Insight Manager.
- Type the server IP address, using port 2301. An example IP address is http://122.18.1.14:2301. The default logon account is anonymous. Click the account name to log on as Administrator. The user name and password are both administrator, lower case. Once logged on as an administrator, the user can change the password.



System Name : D004DKN1K022-

Manually Refreshed @ 05/26/2000 11:13:07

System Board

Product Name:	TaskSmart N2400
ROM Version:	05/04/2000, Family 386S5, Type 03
ROM Diags:	N/A
Hours in Service:	45
Serial Number:	D004DKN1K022
Bus Type:	PCI

CPUs

Processor:	✓ Pentium III /733Mhz	**Action:**	No Action Needed
Coprocessor:	Integrated FPU /733Mhz	**Cache:**	L2 256 KB

Figure 5-3. Compaq Insight Manager Agent Web interface

For more information about Compaq Insight Manager, see the Compaq Management CD.

Enterprise Management Applications

The following enterprise management applications are not directly installed onto the TaskSmart N2400 appliance, rather they are installed onto the client machine.

HP OpenView (Windows 2000 Operating System)

The TaskSmart N2400 appliance can be managed using HP OpenView by following these steps:

1. Install Compaq Insight Manager for HP OpenView Version 2.0 or higher.
2. Modify *CPQCONFIG.DAT* in HP OpenView.

Compaq Insight Manager for HP OpenView, Version 2.0

Compaq Insight Manager for HP OpenView integrates Compaq hardware management and event notification into the HP OpenView Network Node Manager (NNM) network management console.

Depending on the version of Compaq Insight Manager for HP OpenView that is being used, an addition to the *CPQCONFIG.DAT* may be needed to manage the TaskSmart N2400 appliance from HP OpenView. Because HP OpenView works with different platforms, the location of the *CPQCONFIG.DAT* file varies. Do a search for the file. When the file has been located, add the following line to the file and save it:

```
Server : ntsrvr : 1.3.6.1.4.1.232.11.2.7.2.1.4.0 string "TaskSmart N2400";
```

This command string allows HP OpenView to identify the TaskSmart N2400 appliance.

Compaq Insight Manager for HP OpenView introduces an integrated browser launch from the NNM console to the home page of the Web-enabled Compaq Management Agents, as shown in Figure 5-4. The interface is used to collect in-depth information about installed Compaq hardware.

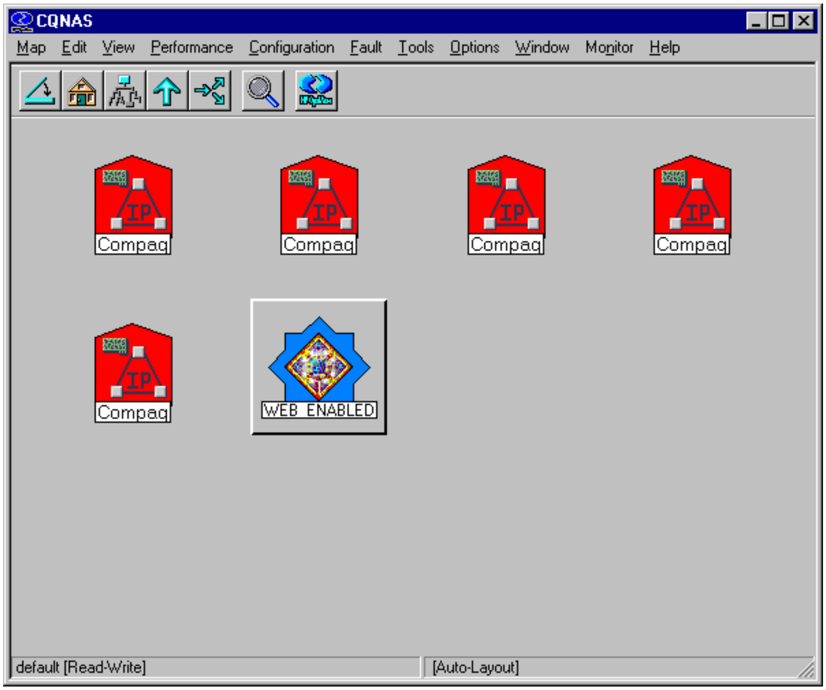


Figure 5-4. Web Enabled interface

The information collected includes system status, system health, prefailure monitors, performance and environmental data, event alarms, and Windows 2000 statistics. Compaq Insight Manager for HP OpenView can be obtained from the Compaq website:

http://www.compaq.com/products/servers

Tivoli NetView (AIX)

The TaskSmart N2400 appliance can be managed using Tivoli NetView (AIX). Several steps are required to be able to manage the TaskSmart N2400 appliance through Tivoli NetView.

1. Install Compaq Insight Manager for Tivoli NetView Version 2.0 or later.
2. Modify *CPQCONFIG.DAT* in Tivoli NetView.

Compaq Insight Manager for Tivoli NetView (AIX), Version 2.0

Compaq Insight Manager for Tivoli NetView integrates Compaq hardware management and event notification into the Tivoli NetView network management console. This release introduces an integrated browser launch from the NetView console to the home page of the Web-enabled Compaq Management Agents, which is used to collect in-depth information about Compaq hardware. The information collected includes system status, system health, prefailure monitors, performance and environmental data, event alarms, and Windows 2000 statistics. Compaq Insight Manager for Tivoli NetView can be obtained from the Compaq website:

http://www.compaq.com/products/servers

Depending on the version of Compaq Insight Manager for Tivoli NetView that is being used, an addition to the *CPQCONFIG.DAT* may be needed to manage the TaskSmart N2400 appliance from Tivoli NetView. Often the location of the *CPQCONFIG.DAT* file varies. Do a search for the file. Once the file has been located, add the following line to the file and save it:

```
Server : ntsrvr : 1.3.6.1.4.1.232.11.2.7.2.1.4.0 string "TaskSmart N2400";
```

This command string allows Tivoli NetView to identify the TaskSmart N2400 appliance.

Installing the Management Software—On the Client Machine

Compaq Insight Manager

1. Insert the Compaq Management CD Version 4.70 or later into the management console.
2. From the Compaq Management CD window, click **Compaq Insight Manager.**
3. Select **Compaq Insight Manager** and follow the installation directions.

Compaq Insight Manager for HP OpenView (Windows 2000 Operating System)

- For detailed instructions on downloading and installing Compaq Insight Manager for HP OpenView (Windows 2000 operating system), visit the following website:

  http://www.compaq.com/products/servers/management/nt-ov-dl.html

- For detailed instructions on downloading and installing Compaq Insight Manager for HP OpenView (HPUX) visit the management area website:

  http://www.compaq.com/products/servers/

Compaq Insight Manager for Tivoli NetView

- For detailed instructions on downloading and installing Compaq Insight Manager for Tivoli NetView (AIX) visit the management area of the Compaq website:

  http://www.compaq.com/products/servers/

Chapter 6

Advanced Administrative Procedures

The Compaq TaskSmart N2400 appliance is preconfigured at the factory with default settings. However, the default settings can be changed to better represent your company needs. This chapter describes step-by-step procedures for configuration and the advanced features of the TaskSmart N2400 appliance listed below:

- Storage Management
- Drive Arrays and Smart Array Controllers
- SANworks Virtual Replicator (SWVR)
- Moving Drives
- Replacing a Failed Drive and Using Spares
- Moving Arrays
- Capacity Expansion
- Ethernet Teaming Features and Procedures
- Using Uninterruptible Power Supplies (UPSs)
- Password Synchronization

Storage Management

The TaskSmart N2400 appliance ships with preconfigured storage settings. This section is intended to assist in the modification of the storage configuration. An overview and step-by-step procedures guide you through creating arrays, pools, and virtual disks. Replacing failed disks and preserving the appliance fault tolerance are also demonstrated in this section.

The lowest level of storage management on the appliance occurs at the physical drive level. Physical drives are placed into the external storage enclosure or enclosures and grouped into RAID arrays for fault tolerance and better performance. Appendix B “RAID Levels” details the benefits provided by RAID arrays. The Array Configuration Utility (ACU), a graphical tool, incorporates a wizard-style interface that creates arrays from the physical drives.

CAUTION: Existing logical drives must not be deleted prior to deleting the virtual disks and pools associated with these logical drives. See “Deleting Virtual Disks and Pools” later in this chapter.

Drive arrays are used to create logical drives, using the ACU. The logical drives are configured as RAID 5 drives for the most efficient fault-tolerant performance. Drives can be added to existing arrays at a later time, forming new logical drives, or they can be added as a new array.

Using Compaq SANworks Virtual Replicator (SWVR), the logical drives created with the ACU become members of a storage pool. Storage pools aggregate the disk space from one or more logical disks into a large set of disk blocks. From the pool of blocks, virtual disks are created, and presented to the operating system as New Technology File System (NTFS) volumes. Virtual drives can be enlarged at a later time when there is a need for more space.

Figure 6-1 is a graphical overview of all storage components used for space management.

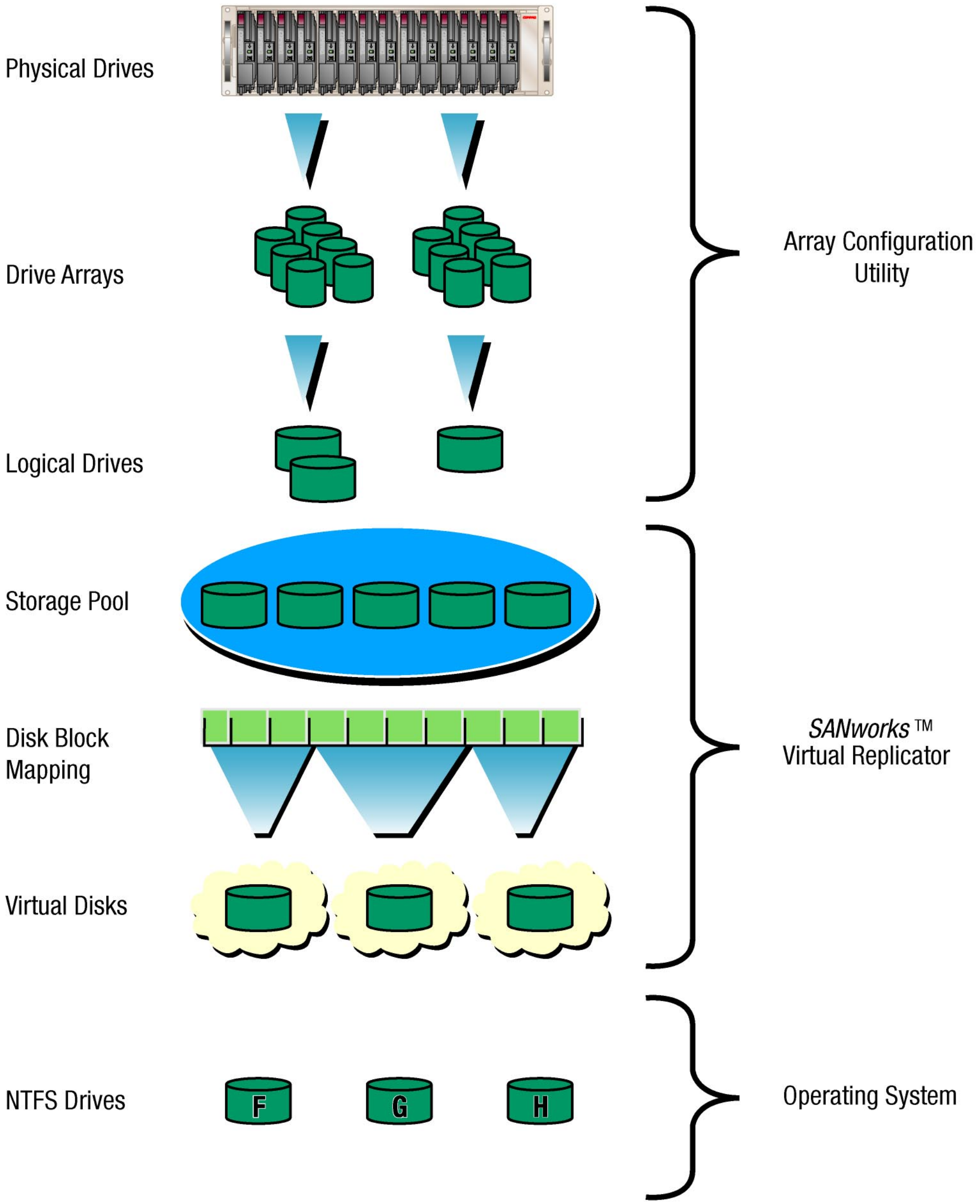


Figure 6-1. Space management process

Drive Arrays and Smart Array Controllers

Array Configuration Utility

The TaskSmart N2400 appliance can have as many as 56 physical drives in up to four external storage enclosures. The drives are arranged in RAID array set groups of up to 14 drives. Drive arrays distribute data across a series of hard drives to unite them into one or more higher performance logical drives. Distributing the data across multiple drives allows the data to be read and written faster. Additionally, arrays can protect against data loss using a number of protection schemes. The Array Configuration Utility (ACU) is used to configure and expand data storage. The ACU is an easy-to-use graphical interface for setting up drive arrays and fault tolerance, and adding storage.

Features of ACU

- Graphical representation of drive array configurations
- Wizards that help optimize array configuration
- Express or custom initial configuration
- Online spare (hot spare) configuration
- Separate fault-tolerant configuration on a logical drive basis
- Easy capacity expansion
- Online stripe size migration
- User-selectable stripe size
- Drive rebuild and capacity expansion priorities

The appliance was configured in the factory with a specific array and logical drive layout based on the number of installed drives, as shown in Table 6-1. The array and logical drive setup is based on the listed defaults. When a full QuickRestore is applied to your system these defaults ease recovery. The QuickRestore utility uses the same defaults to decide how installed drives are set up in arrays and logical drives. Refer to Appendix C, “Troubleshooting,” for more information about the QuickRestore utility.

Table 6-1
Data Drive Groups

Number of Storage Enclosures	Number of Drives	Drives Lost to RAID 5 Arrays	Number of RAID 5 Arrays
1	4 to 14	1	1
2	15 to 28	2	2
3	29 to 42	3	3
4	43 to 56	4	4

Array Controllers

Inside the TaskSmart N2400 appliance, there are two separate RAID array controllers. The Integrated Smart Array Controller protects the operating system drives in the server, using RAID 1. The four-port Smart Array Controller guards the data drives in the external enclosures, using RAID 5 (distributed data guarding) for fault-tolerant data protection. The Smart Array Controller provides high performance RAID functionality for the data drives. For a more thorough discussion of RAID levels and how they protect your data, refer to Appendix B.

Key Features and Benefits of the Smart Array Controller

- **Four channels—**four external SCSI channels, each supporting up to fourteen 36.4-GB disks.
- **128-MB error checking and correcting (ECC)—**cache memory, battery-backed and removable
- **Ultra3 SCSI—**up to 160 MB per channel
- **New Performance Architecture—**with 64-bit RISC processor engine
- **64-bit PCI design**
- **Compaq Pre-Failure Warranty—**support for hard drives (requires Compaq Insight Manager)
- **Online management features—**online capacity expansion, online stripe size migration, online spare (global)

- **Onboard rechargeable batteries—**The array accelerator is backed up so that data temporarily held there (cached) is safe during equipment failure or power outage. Backup is particularly important for data that has been cached by a posted-write but has not yet been written to the hard drives. The batteries preserve data in the array accelerator for a minimum of four days.

IMPORTANT: The rechargeable batteries on a new Smart Array Controller can be discharged when the board is first installed. During server power-up with discharged array accelerator batteries, Power-On-Self-Test (POST) displays the code “1794,” indicating that the array accelerator is disabled. This error message does not require action. The array accelerator is automatically enabled when batteries are charged to 90 percent of their capacity.

The internal circuitry can take up to 36 hours to fully charge the batteries. During this time, the array accelerator is disabled, but the Smart Array Controller properly functions, without the performance advantage of the array accelerator.

Managing Drive Arrays Using ACU

The ACU is an intuitive graphical tool. With configuration wizards, your array controller is set up and ready to use in minutes. Changing the default configuration of the TaskSmart N2400 appliance is optional.

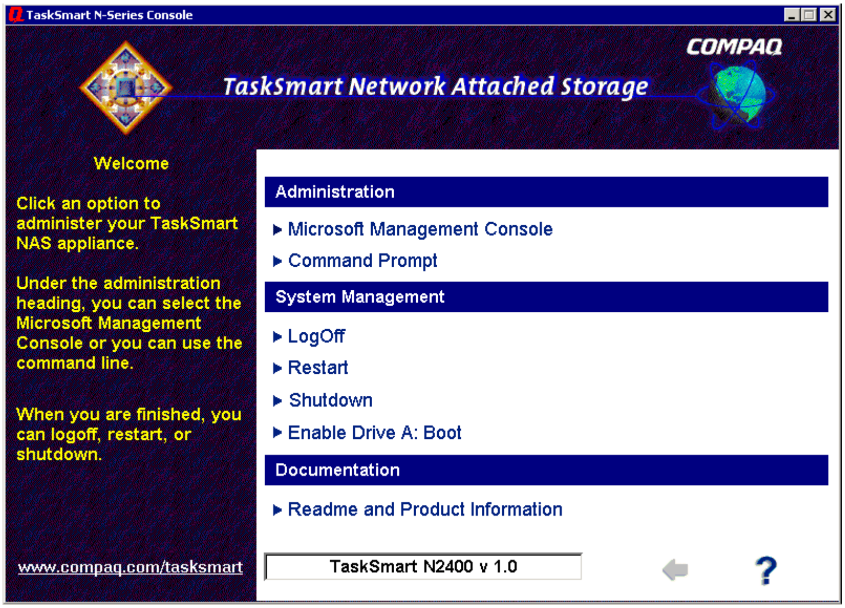
Creating Arrays

The ACU provides a wizard-type interface for creating or modifying drive arrays. Some of the most important features of the ACU include:

- Graphical representation of drive arrays and physical disks
- Express or custom configurations
- Online spare (hot spare) configuration
- Easy capacity expansion
- Selectable drive rebuild and array expansion priorities

Change your array configuration, set up a new array, or add drives to an existing array by using the following procedure:

1. Log on to the TaskSmart N2400 appliance as Administrator.
2. From the TaskSmart N2400 console, click **Microsoft Management Console.**



Welcome

Click an option to administer your TaskSmart NAS appliance.

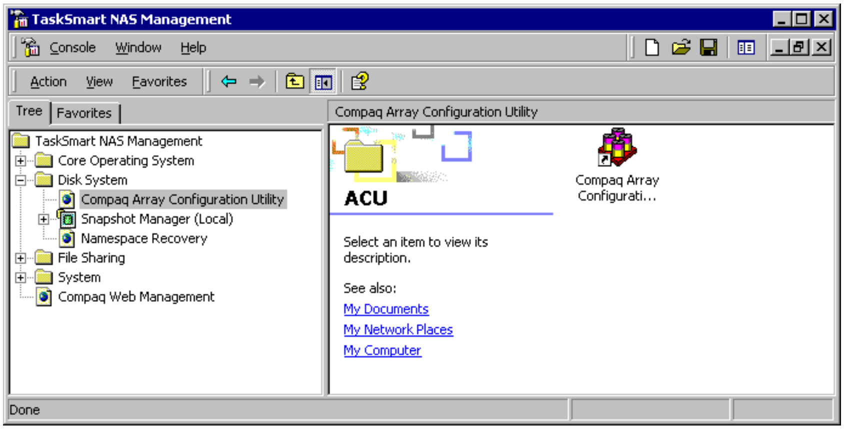
Under the administration heading, you can select the Microsoft Management Console or you can use the command line.

When you are finished, you can logoff, restart, or shutdown.

Figure 6-2. TaskSmart N2400 console screen

3. Expand the **Disk System** folder.

4. Click **Compaq Array Configuration Utility** to open the ACU.
5. Double-click the **Compaq Array Configuration Utility** icon in the right pane of the interface to launch the ACU.

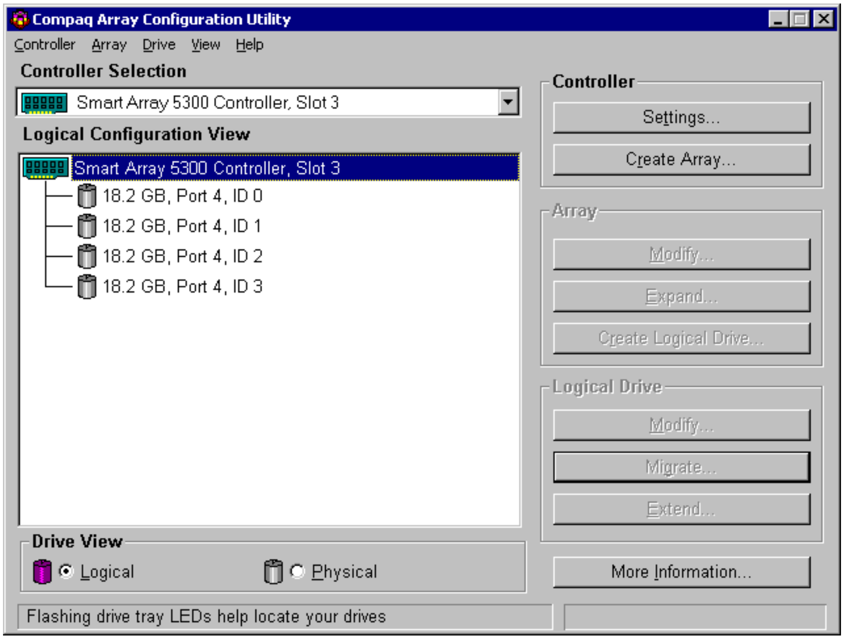


Select an item to view its description.

See also:

Figure 6-3. Compaq System Tools menu selection screen

6. Under Controller Selection, click the drop-down box, and then select **Smart Array 5300 Controller.**
7. The ACU presents either a physical or logical view of the arrays and drives. The view is selectable using the option buttons at the bottom of the interface. Select **Logical,** and then click **Create Array.**



Controller Selection: Smart Array 5300 Controller, Slot 3

Smart Array 5300 Controller, Slot 3
- 18.2 GB, Port 4, ID 0
- 18.2 GB, Port 4, ID 1
- 18.2 GB, Port 4, ID 2
- 18.2 GB, Port 4, ID 3

Drive View: ● Logical ○ Physical

Flashing drive tray LEDs help locate your drives

Figure 6-4. Smart Array Controller Configuration Utility preview dialog box

IMPORTANT: Be sure to select the array controller after you start the ACU. Make sure that the array controller displayed at the top of the window is NOT the Integrated Smart Array Controller. Changes to the configuration of the controller can corrupt the operating system on the server.

CAUTION: Existing logical drives must not be deleted prior to deleting the virtual disks and pools associated with these logical drives. See “Deleting Virtual Disks and Pools” later in this chapter.

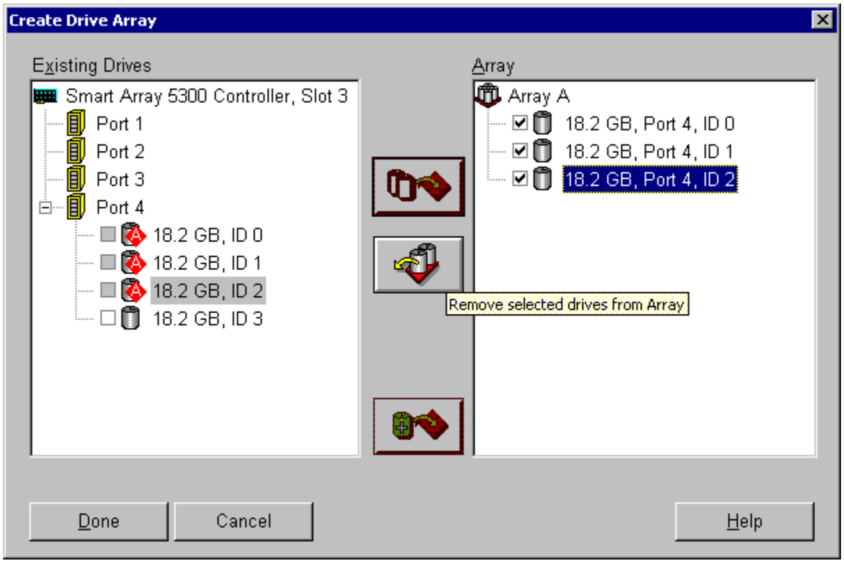
8. Select the physical drive or drives that you would like to include in the new array.

   NOTE: Compaq recommends that an array set for RAID 5 consist of a maximum of 14 physical drives. The more member drives in an array, the greater the chance for multidrive failures.

   NOTE: If you are adding drives to an existing array, Compaq recommends that you add the drives in multiples of three or four. The new drives become separate logical drives, as described in the next section.

   NOTE: The maximum number of storage units (logical drives) in a pool is eight. Therefore, it is advantageous to make logical drives as large as possible, if you want to have large pools from which to create virtual disks.

9. Next, click the icon showing the **right-pointing arrow.** All selected drives are then moved into the right pane on the interface, designating their inclusion in a new array.



- Smart Array 5300 Controller, Slot 3
  - Port 1
  - Port 2
  - Port 3
  - Port 4
    - ☐ 18.2 GB, ID 0
    - ☐ 18.2 GB, ID 1
    - ☐ 18.2 GB, ID 2
    - ☐ 18.2 GB, ID 3

- Array A
  - ☑ 18.2 GB, Port 4, ID 0
  - ☑ 18.2 GB, Port 4, ID 1
  - ☑ 18.2 GB, Port 4, ID 2

Figure 6-5. Create Drive Array A screen

10. Compaq recommends that you designate a spare drive for your array. This online spare, or “hot spare,” is automatically used immediately when one of the other member drives in the array fails. When a failure is detected, the array controller uses parity information to rebuild the information that was on the failed drive. After the rebuilding process, the array resumes its fault-tolerant state. If you do not have a spare drive for your array and a drive fails, you are unable to begin rebuilding until you physically replace the failed drive. Until the drive is replaced and the rebuild process is complete, the array is not fault tolerant. If another drive fails at this time, data loss is probable. To select a spare drive, use the spare drive icon located at the bottom of the screen and add the drive to the array set. Spares can be shared among arrays.
11. You have now completed your array configuration. Once complete, you must create a logical drive before exiting or the new array will not be saved. Use the procedure in the next section to create a logical drive or drives from your arrays.

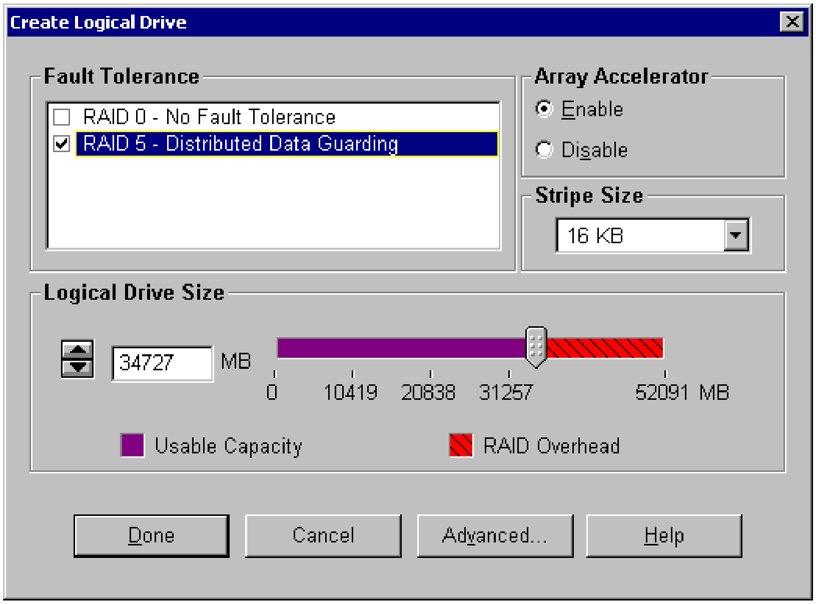
Creating Logical Drives from Arrays

Now that you have gathered your physical drives into fault-tolerant arrays, you need to create logical drives from them. You can choose to create one large logical drive using the entire space of the array, or you may want to divide each physical drive into two or more logical drives. Compaq recommends that you create one logical drive from the array. You can add physical drives to the array later.

Procedure:

1. Log on to the TaskSmart N2400 Appliance as Administrator.
2. From the TaskSmart N2400 console, click **Microsoft Management Console.**
3. Expand **Disk System** folder.
4. Click **Compaq Array Configuration Utility.**
5. In the right pane of the interface, double-click the icon to start the Compaq Array Configuration Utility.
6. Be sure that the Smart Array 5300 Controller is selected at the top of the interface (do not select the integrated one).
7. Select an array from which to create the logical drive.
8. Click the **Create Logical Drive** button.

9. In the upper left area of this screen, select **(RAID 5) Distributed Data Guarding,** which provides the most efficient fault-tolerant protection for your data.



Create Logical Drive

Fault Tolerance

☐ RAID 0 - No Fault Tolerance
☑ RAID 5 - Distributed Data Guarding

Array Accelerator

● Enable
○ Disable

Stripe Size: 16 KB

Logical Drive Size: 34727 MB

Figure 6-6. Create Logical Drive dialog box

10. Be sure that the array accelerator is enabled.

11. Set stripe size to desired value.

12. Set the logical drive size. Use the default values to create a logical drive that occupies the entire array.

13. Click **Done.**

14. If you have other arrays, repeat the procedure to create new logical drives on those arrays as well.

15. You must rescan the drives so that the newly created logical drives are visible to the operating system. This procedure is accomplished from the TaskSmart N2400 console. To find the newly created logical drives:
    a. Right-click the **My Computer** icon on the desktop.
    b. Select **Manage** from the menu.
    c. Double-click **Device Manager.**
    d. Right-click **Disk Drives,** and then select **scan for hardware changes.**

16. After you have set up your arrays and logical drives, you must add the logical drives into a pool of space from which virtual disks can be created. Use the information in the next section to learn about pools and virtual disks.

CAUTION: SWVR does not support changing the size of a logical drive or logical unit number (LUN) once it has been incorporated into a pool. You must modify an existing array or add a new array. Changing the logical drive size will result in data loss.

CAUTION: The Windows Powered OS Logical Volume Manager (LVM) is not necessary for use with the TaskSmart N2400 appliance and has been disabled. LVM and the use of any active component of SWVR can cause data loss and unexpected behavior. Should the use of LVM be necessary, all SWVR interfaces must be closed prior to and during use. To activate the LVM, refer to the release notes provided with the appliance.

SANworks Virtual Replicator

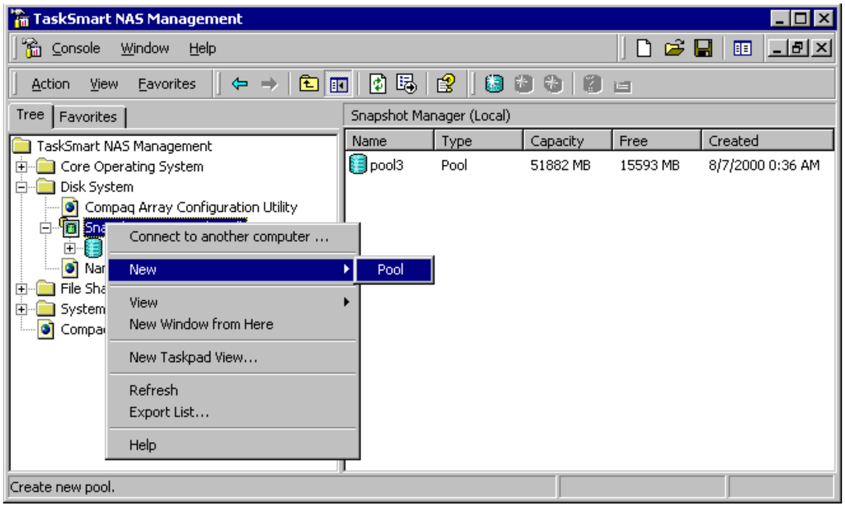
SANworks Virtual Replicator (SWVR) is a Compaq utility for managing disk space logically and efficiently. SWVR combines logical drives into a pool of space, from which the administrator can create virtual disks of exactly the correct size needed by a particular group or user. The virtual disks can be expanded later, so this virtualization is a very powerful administrator tool.

Creating Pools Using SWVR

The process of creating a pool of disk space and dividing it into virtual disks is straightforward.

1. Log on as Administrator.
2. From the TaskSmart N2400 console, click **Microsoft Management Console.**
3. Click **Disk System.**
4. Click **Snapshot Manager (Local),** which controls pools, virtual disks, and snapshots. Snapshots are discussed in Chapter 3, “Windows File System Administration.”

5. In the Snapshot Manager interface, right-click Snapshot Manager, select **New,** and then click **Pool.**



Name	Type	Capacity	Free	Created
pool3	Pool	51882 MB	15593 MB	8/7/2000 0:36 AM

Figure 6-7. Snapshot Manager screen

6. The New Pool Wizard starts and the logical drives are displayed that are available to be included in new pools.

NOTE: When creating pools or virtual disks, the wizard progresses to the final screen prior to checking for duplicate names of a pool or virtual disk. The wizard gives an error message if duplicate names exist, and then exits. To correct the error, the wizard must be restarted.

7. Select an available storage unit or units (logical drives) to include in your new pool, and then click the **right-pointing arrow button** in the center of the interface to move the drive into your new pool. Repeat this process for each logical drive that you want to include.

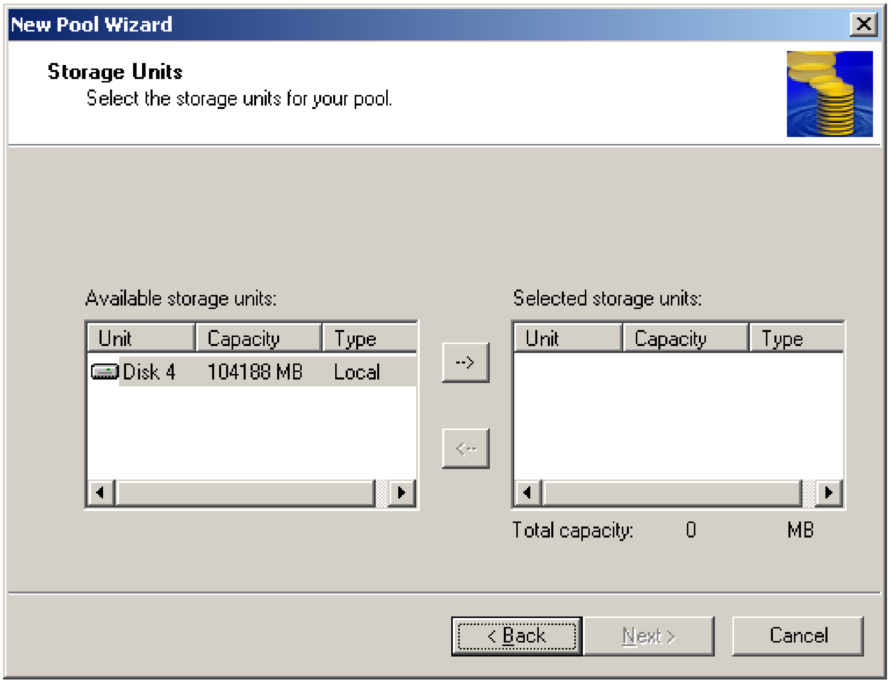


Figure 6-8. Selected Logical Drives dialog box

NOTE: You can have up to eight logical drives as members of a pool.

8. Click **Next** to proceed.
9. Select the segment size of your pool, noting that this selection determines the maximum size of a virtual disk that may be created in the pool. Compaq recommends a segment size of 128 KB.

   You can see the total capacity of your new pool displayed at the bottom of the right pane.
10. Click **Next,** and then click **Finish.**

Creating Virtual Disks from Pools

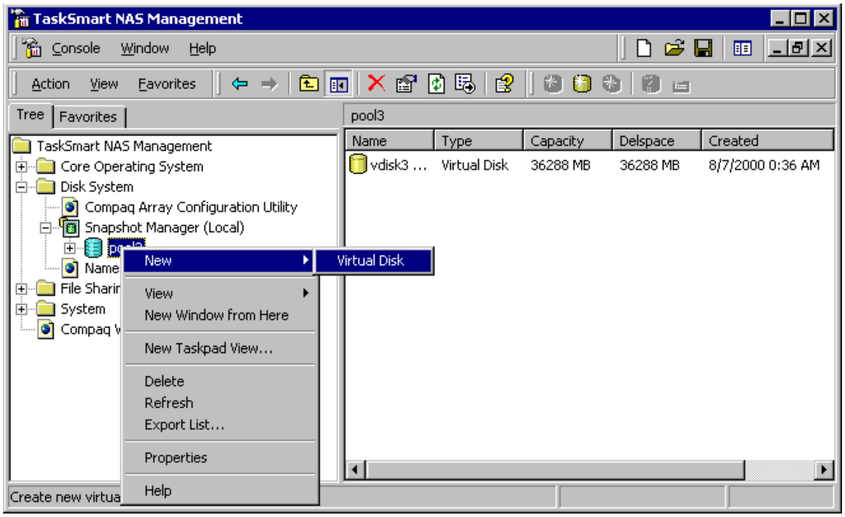
Virtual disks are the storage entities that the operating system recognizes as drives, and upon which your data is placed. Because virtual disks are created from pools, they can be made exactly the size that you need them to be. From a pool, you may wish to create three separate virtual disks that exactly match the space needs of the users or groups requesting space, or you may create a single, large virtual disk from a pool. A limitation is that virtual disks may not “span” pools—they must be created from a single pool.

NOTE: Your pool has a “reserved” area for snapshot creation. A snapshot is a real-time copy of data on a virtual disk.

NOTE: By default, 30 percent of your pool space is devoted to snapshot reserves. Depending on how fast your data changes and the number of snapshots that you keep, you may need more or less space devoted to snapshots.

Procedure:

1. In the Snapshot Manager interface, right-click on a pool, and select **New Virtual Disk.**



pool3

Name	Type	Capacity	Delspace	Created
vdisk3 …	Virtual Disk	36288 MB	36288 MB	8/7/2000 0:36 AM

Figure 6-9. Snapshot Manager interface

2. The New Virtual Disk Wizard pops up and guides you through the creation process.
3. Assign a drive letter to each virtual disk that you create to make it accessible to the operating system.
4. Format the virtual disk, using the recommended 16-KB allocation unit size, or a size slightly larger than the average file size.

IMPORTANT: Using the 16-KB allocation unit size is recommended for optimum performance. However, disk defragmentation software does not operate properly. See “Snapshots and Drive Defragmentation” in Chapter 2, “Administrative Procedures,” for more information.

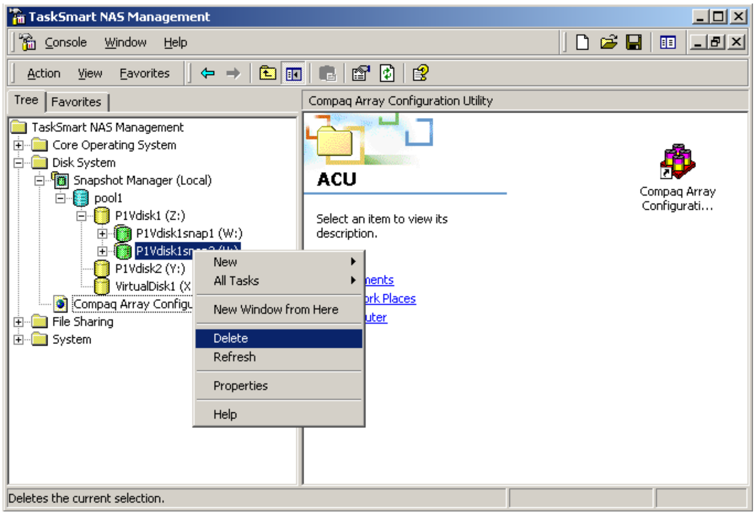
Deleting Virtual Disks and Pools

When deleting virtual disks, it is important to remember the following:

- Virtual disks must be deleted from the SWVR Snapshot Manager before the underlying disk structure is deleted.
- Do not delete the logical drives from the ACU before deleting the virtual disks.
- You must delete all the snapshots associated with a virtual disk before you can delete the virtual disk.
- If the virtual disk contains any data that you want to keep, back up the data. Deleting a virtual disk destroys all the data stored on the disk.
- Make sure that no one is accessing the virtual disk. You cannot it delete if any files on the disk are open.

To delete a virtual disk:

1. From the TaskSmart N2400 console, click **Microsoft Management Console,** click **Disk System,** and then click **Snapshot Manager.**
2. Expand the list showing pools, virtual disks, and snapshots.
3. Right-click any snapshots that are associated with the virtual disk to be deleted, and then select **Delete.** Click **OK.** Repeat this step until there are no snapshots associated with the virtual disk.

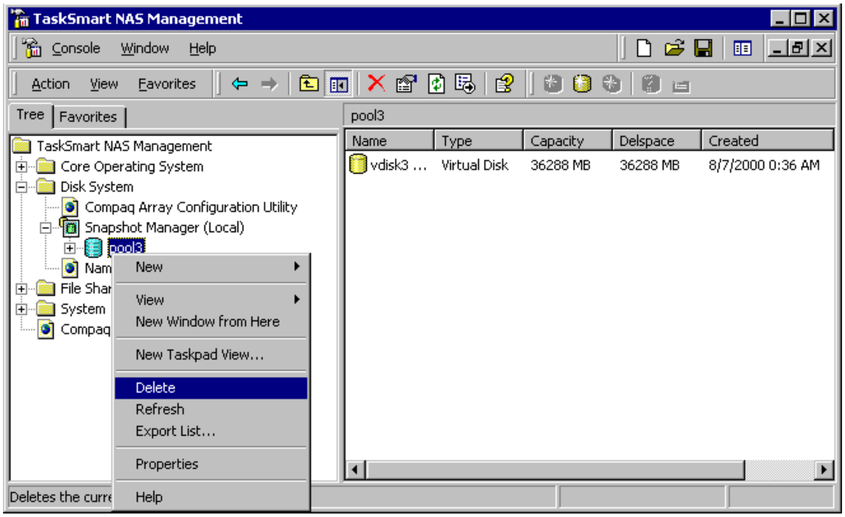


Select an item to view its description.

Deletes the current selection.

Figure 6-10. Snapshot Manager screen, deleting snapshots

4. Select the virtual disk to be deleted, and then right-click **Delete.**



Name	Type	Capacity	Delspace	Created
vdisk3 …	Virtual Disk	36288 MB	36288 MB	8/7/2000 0:36 AM

Figure 6-11. Snapshot Manager screen, deleting a virtual disk

5. Click **OK** to confirm that you want to delete the virtual disk and erase all the data stored on it.

NOTE: When you delete a virtual disk, make sure to delete any scheduled tasks for the disk. Otherwise, if you reuse the old virtual disk name for another virtual disk, the old tasks run on the new disk. Use the Windows Scheduled Tasks applet to delete scheduled tasks.

6. Select the pool to be deleted, and then right-click **Delete.**
7. Click **OK** to confirm that you want to delete the pool and erase all the data stored in it.

Online Volume Growth

The SWVR online volume growth feature directs the operating system to update the size of a physical drive or virtual disk without requiring a system restart. Online volume growth can also instruct the operating system to grow the on-disk partition information for a volume. This feature allows a volume to grow into unused space made available by either increasing the size of a drive or by deleting one or more adjacent partitions. With online volume growth, you can increase storage capacity, as required by your users and applications, easily and with zero downtime.

Preparing for Online Volume Growth of Basic or Virtual Disks

Before growing a volume, review the following checklist:

- Make a reliable backup copy of the data. If the drive that you plan to grow contains any data that you want to keep, it is recommended that you back up the data.
- Plan for new storage. Adding capacity can increase the time required to create backups.
- Before performing online volume growth, make sure that the pools that you have created have adequate free space. When you increase the size of a virtual disk, it consumes more space in the pool and reduces the amount of free space that can be used for snapshots of virtual disks.
- When replacing hard drives or using the ACU to perform array expansion, the controller must finish rebuilding/expanding/extending before online volume growth can be performed.
- Using the ACU to modify an array takes time. Examine the current controller rebuild/expand priority settings. See the documentation for the Compaq Array Configuration Utility.

Adding Additional Storage Units to the Pool

Before you can grow a volume, you may need to add additional storage units. If this is the case, you must first add additional physical drives, add them to an array or create a new array, create a new logical drive and then add it to the pool. See the section "Capacity Expansion," later in this chapter for additional information.

CAUTION: SWVR does not support changing the size of a logical drive or logical unit number (LUN) after it has been incorporated into a pool. You must modify an existing array or add a new array. Changing the logical drive size will result in data loss.

When the additional drives are available, add them to the existing array.

1. Access the ACU.
2. If this results in launching a Wizard, cancel the wizard and follow these steps.
3. Under Controller Selection, click the drop-down box and select **Smart Array 5300 Controller**.
4. You can modify an existing array up to a total of 14 drives for the array by clicking the desired array, and then clicking **Modify**. Optionally, if you added a sufficient number of physical drives, you can create a new array by clicking **Create Array**.
5. Select the additional drives to be added to the array and assign them to the array.
6. Click **Done** and then click the unused space for the array.
7. Click **Create Logical Drive**, select the desired raid type, and then click **Done**.
8. Save the array configuration.

   NOTE: If you modified an existing array, you must wait for the rebuild to complete. The new logical drives will not be available to the OS until the rebuild process completes.

9. Using Windows Device Manager, rescan for the new drive.

Next, add the New Logical Drive to the Pool.

IMPORTANT: The user can add a maximum of eight logical drives to a pool.

---

1. From the TaskSmart N2400 console, click **Microsoft Management Console**.
2. Click **Disk System,** and then click **Snapshot Manager**.
3. Select the desired pool.
4. Right-click **Properties** to show the Pool Properties dialog box.
5. Click the **Storage Units** tab, and then click **Add.** The Add New Storage Units screen is displayed.
6. Select the storage unit you want to add, and then click **Add.**
7. Click **OK** to dismiss the pop-up that tells you that the storage units have been added to the pool.
8. Click **OK** to dismiss the Pool Properties screen.

Growing a Virtual Disk Volume

The following procedure explains how to grow a virtual disk volume when using the Microsoft Management Console (MMC) interface. This procedure assumes that there is adequate space available in the pool. If space is not available, see the previous section on adding additional storage units to the pool.

> **NOTE:** Drive volume growth must not be performed at the same time as other major drive management operations.

To grow a virtual disk volume:

1. From the TaskSmart N2400 console, click **Microsoft Management Console.**
2. Click **Disk System,** and then click **Snapshot Manager.**
3. Select the desired pool.
4. Right-click the virtual disk that you want to grow, and then select **All Tasks.**
5. Select **Grow Volume.**
6. The welcome screen of the Grow Volume Wizard is displayed. Click **Next** to start the wizard.
7. In the Virtual Disk Information dialog box, confirm that the specified virtual disk is the one that you want to grow. If not, click **Back** and repeat step 4 to select the correct virtual disk, or click **Next** to proceed.

> **NOTE:** Online volume growth operates only on virtual disks formatted with New Technology File System (NTFS). If the file system is not NTFS, the wizard presents an error message and instructs you to cancel.

8. In the Set New Volume Size dialog box, specify the amount by which you want the virtual disk to increase. The Megabytes available field shows available pool space.

9. Specify the growth amount in the Megabytes to grow box, or in the Percentage to grow box, or by using the slider control.

   NOTE: The amount of free space shown includes the default 30 percent free pool space reserved for snapshots. Online volume growth does not grow the volume beyond the amount of free pool space reserved. If you attempt to grow the volume beyond the reserved space, an error occurs.

   NOTE: When using Snapshot Manager for online volume growth, the smallest amount that a virtual disk can be grown is 1 MB.

10. Click **Next.**
11. In the Confirm Selected Volume dialog box, confirm online growth for the specified virtual disk. If you want to make changes, click **Back.** If you want to proceed with online volume growth, click **Next.**
12. After the virtual disk size increases to its new size, click **Finish** to close the wizard.

Online volume growth for virtual disks is also possible using the Online Volume Growth Wizard from the Microsoft Management Console.

1. Log on to the TaskSmart N2400 appliance as Administrator.
2. Click **Microsoft Management Console.**
3. Click the **Compaq Web Management** folder to see the Native Administration Methods table.
4. Click **Other Tools.**
5. From the Windows Explorer interface, select the **My Computer** folder, then right-click on the volume, and then select the Online Volume Growth tab.

Moving Drives

CAUTION: All data must be backed up before removing drives or changing configurations. Failure to do so could result in permanent loss of data. The system must be powered down.

Drives in the external storage enclosures can be moved, but you should do this only after a complete and successful backup, and when the appliance has been powered down and turned off. To move drives, the following conditions must be met:

- System is powered down (includes all system components).
- No drive failures are identified. The array must be in its original configuration.
- Capacity expansion or drive rebuild is not in progress.
- Controller firmware is the latest version (recommended).

When the above conditions are met, move the drives using the following procedure:

1. Remove one drive at a time by unlatching and sliding it out of the drive bay about one inch.

IMPORTANT: Before you remove a drive from the drive bay, be sure to allow a few seconds for the drive to completely spin down before handling it. If you have completely powered down the external enclosure, the drives should already have spun down.

2. Move the drive to the desired location in an external storage enclosure.
3. Restore power to the external storage enclosure or enclosures, and then power up the server. As the system restarts, you should see a 1724 POST message, indicating that the drive positions have changed and are updated. If a 1785 POST message is displayed, immediately power down the system components to prevent data loss and return each drive to its original location. Then power up the server as usual.
4. Run the ACU if you wish to view and confirm the new drive positions.

When moving drives, refer to Table 6-3, “Storage Enclosure Drive Bay Configuration,” later in this chapter.

CAUTION: All data must be backed up before removing drives or changing configurations. Failure to do so could result in permanent loss of data. The system must be powered down before removing drives.

Replacing a Failed Drive and Using Spares

The TaskSmart N2400 appliance is designed with many fault-tolerant features to prevent common problems. However, if a drive fails, it must be replaced. Because your external drives are set up in RAID 5 arrays with distributed data guarding, the loss of a single drive in an array does not result in any loss of data. However, you must replace the failed drive as soon as possible. Until a failed drive is replaced, your TaskSmart N2400 appliance is operating in a non-fault-tolerant mode. If another drive is lost before the failed one is replaced and rebuilt, you can lose all data on the array.

NOTE: Refer to the maintenance and service guide for detailed procedures about hardware failures on the TaskSmart N2400 appliance.

Failed drives can be replaced without the server being powered down. The drives in your server are hot-pluggable. To identify failed drives, look for one or more of the following:

- An amber LED is illuminated on a failed drive. This LED indicates that the storage enclosure is powered up and that the SCSI cable connecting the storage enclosure to the server is working.

  NOTE: The amber light may briefly illuminate when the drives are inserted. This illumination is normal and does not indicate a failure condition unless the LED remains illuminated.

- An amber LED is illuminated on the storage enclosure. This LED indicates that one or more drives in the storage enclosure has failed, a fan failure has occurred, or a high-temperature condition exists.
- A (POST) message lists failed drives when the TaskSmart N2400 appliance is restarted. This message is dependent on the array controller detecting one or more “good” drives.
- The Array Diagnostics Utility (ADU), found on the SmartStart and Support Software CD, reports failed drives.
- The Compaq Insight Manager reports failed drives or prefailure conditions on one or more drives.

Hard Drive LED Indicators

The hard drive LEDs, located on each physical drive, are visible on the front of the server or on the front of the storage enclosure. They provide activity, online, and fault status for each corresponding drive when configured as a part of an array and connected to a powered-up controller. LED behavior can vary depending on the status of other drives in the array.

This section provides the following information about hard drive LEDs:

- An illustration detailing the location of each LED
- A table of the possible LED configurations and what each combination means

CAUTION: Read "Hot-Plug Drive Replacement Guidelines" in the *Compaq Servers Troubleshooting Guide* before removing a hard drive.

For additional information on troubleshooting hard drive problems, refer to "Hard Drive Problems" and "SCSI Device Problems" in the *Compaq Servers Troubleshooting Guide*.

Use the following illustration in conjunction with Table 6-2 to analyze current statuses for hot-plug hard drives that are connected to a Compaq Smart Array Controller.

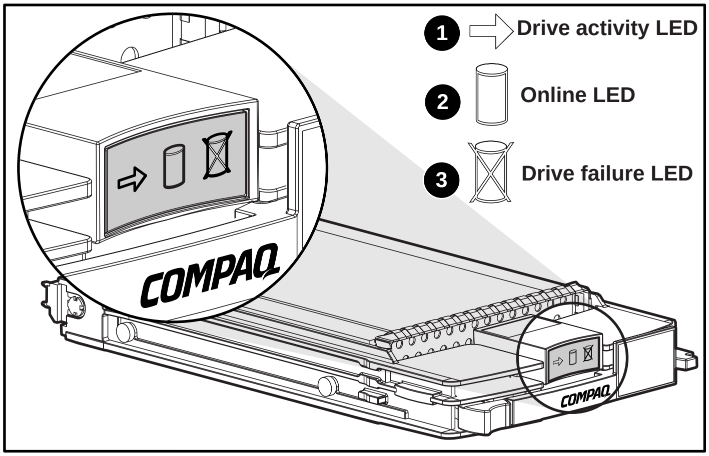


Figure 6-12. Hot-plug hard drive LED indicators,

Table 6-2
Hard Drive LED Combinations

❶ Activity	❷ Online	❸ Drive Failure	Indication
△ **CAUTION:** Read “Hot-Plug Drive Replacement Guidelines” in the *Compaq Servers Troubleshooting Guide* before removing a hard drive.			
On	Off	Off	**Do not remove the drive. Removing a drive during this process causes data loss.** The drive is being accessed and is not configured as part of an array.
On	Flashing	Off	**Do not remove the drive. Removing a drive during this process causes data loss.** The drive is rebuilding or undergoing capacity expansion.
Flashing	Flashing	Flashing	**Do not remove the drive. Removing a drive during this process causes data loss.** The drive is part of an array being selected by the ACU. -Or- The Options ROMPaq™ is upgrading the drive.
Off	Off	Off	OK to replace the drive online if a predictive failure alert is received (see the “Predictive Failure Alert” section in *Compaq Servers Troubleshooting Guide* for details) and the drive is connected to an array controller. The drive is not configured as part of an array. -Or- If this drive is part of an array, then a powered-up controller is not accessing the drive. -Or- The drive is configured as an online spare.

continued

Table 6-2
Hard Drive LED Combinations *continued*

❶ Activity	❷ Online	❸ Fault	Indication
Off	Off	On	OK to replace the drive online. The drive has failed and has been placed offline.
Off	On	Off	OK to replace the drive online if a predictive failure alert is received (see the “Predictive Failure Alert” section in *Compaq Servers Troubleshooting Guide* for details), provided that the array is configured for fault tolerance and all other drives in the array are online. The drive is online and configured as part of an array.
On or flashing	On	Off	OK to replace the drive online if a predictive failure alert is received (see the “Predictive Failure Alert” section in *Compaq Servers Troubleshooting Guide* for details), provided that the array is configured for fault tolerance and all other drives in the array are online. The drive is online and being accessed.

Replacing Failed Hard Drive Process

Follow this procedure to replace a failed drive:

1. Determine the position of the failed drive. A lighted LED indicator means that the drive has failed. If you are identifying drives by drive number, refer to the following table showing how bay numbers correspond to SCSI ID numbers. It is imperative to identify the correct drive before starting the replacement procedure.

NOTE: All Compaq utilities report drive information in terms of SCSI ID. Only the physical drive enclosure is labeled by bay number. Use Table 6-3 to properly identify the appropriate drive bay.

IMPORTANT: Compaq utilities report drive state through the SCSI ID. Table 6-3 assists you in associating the appropriate drive bay to the corresponding SCSI ID.

Table 6-3
Storage Enclosure Drive Bay Configuration for Replacing Failed Hard Drives

Description														
Bay Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14
SCSI ID	0	1	2	3	4	5	8	9	10	11	12	13	14	15

2. Remove the failed drive by unlatching and sliding it out of the drive bay about one inch.
3. Allow a few seconds for the drive to spin down before removing it completely.

△ **CAUTION:** Be sure to use a drive bay blank to cover open bays if you do not plan to insert a new drive within a few seconds. The drive bay blanks are necessary to maintain proper airflow for cooling. Failure to cover open bays can lead to thermal failure of your drives and loss of data.

4. Insert a new drive of the same type into the bay where the failed drive was located.

Using Spare Drives

To greatly increase the fault tolerance of your TaskSmart N2400 appliance, Compaq recommends that you use at least one of the drives in the storage enclosures as an online spare drive. Using the recommended configuration of RAID 5 (distributed data guarding) on the external enclosure drives, in combination with an online or hot spare, achieves the highest level of protection. In case of a drive failure, an online spare is assigned to an array. If the spare is available, it acts as an immediate replacement for the failed drive. Recovery operations start automatically to rebuild the information from the failed drive onto the spare drive, using the remaining drives and the distributed data guarding (parity) information.

NOTE: Until the rebuild process is complete, a spare drive cannot prevent the failure of the entire array if another drive in the array fails. Additionally, it is possible that noncorrectable drive errors can prevent a successful rebuild operation in some cases.

You can assign a single online spare drive to multiple arrays, or you can choose to devote multiple drives to online spare duty for maximum redundancy. When using a single online spare drive, be sure to assign it to each array in the storage enclosure. The original online spare drive remains a part of the array until the replacement drive is installed. Replacing an online spare drive maintains a high level of fault tolerance.

Compromised Fault Tolerance

If the fault tolerance of an array is compromised due to multiple concurrent drive failures, the condition of the logical drive or drives on that array is “failed,” and unrecoverable errors are returned to the operating system. Data loss is probable. Inserting replacement drives at this time does not improve the condition of the logical drive or drives.

If you encounter this situation, first try powering down the entire system and then powering up. Then remove power from both the server and storage enclosure. Reapply power to the storage enclosure, then the server, and then restart the system. In some cases, a drive with intermittent problems can work long enough for you to make copies of important files. If a 1779 POST message is displayed, press the **F2** key to re-enable the logical drive or drives. Remember, it is likely that data loss has occurred, and any data on a failed logical drive is suspect.

Fault tolerance can also be compromised due to nondrive issues. These issues include faulty SCSI and power cables, power supplies, facility power, or accidental unplugging of storage enclosure power. In such cases, the physical drives in the storage enclosures need not be replaced. However, data loss is possible.

In cases of actual drive failure, replace any drives that have failed to prevent further problems. Afterwards, the fault tolerance may again be compromised, power may need to be recycled, and the 1779 POST message may again be displayed. Press the **F2** key to re-enable the logical drive or drives. Then recreate your pools and virtual disks, and restore data from backup media.

Moving Arrays

If your company has multiple appliances, situations may arise in which you want to move an entire array from one server to another. Because the data on the servers is stored in virtual disks created from drive space pools that may contain space from multiple arrays, you must be careful when moving arrays. The following guidelines are provided:

- If you move an array that has logical drives that are a member of a pool, you must move all other arrays that have logical drives that are also a member of the pool.
- Move all drives in the array at the same time.
- Ensure that no failed drives are present or that no rebuild processes are in progress.
- Ensure that the positions of other drives on the system to which the array is being moved are not being changed at the same time.
- Make a full backup of all data on the server from which the array is being moved before starting the move process.
- Use the ACU to identify which drives are in the array that you wish to move. In the ACU interface, highlighting the array causes the drive lights to flash on the member disks of the array.
- To move the array, power down the system, and unplug power from the server. Then, remove power from the storage enclosure or enclosures and carefully remove the drives.

⚠ **CAUTION:** To avoid data loss, replace failed drives according to configuration guidelines in Table 6-3.

Capacity Expansion

The TaskSmart N2400 appliance is designed for expansion. You can add up to four external storage enclosures to the system for a total of 56 external data drives. Depending on your needs, many configuration options are available:

- Add new drives to an existing array, and create a new logical drive or drives
- Add new drives, create a new array, and create a new logical drive or drives
- Add the new logical drive or drives to existing pool or pools
- Create a new pool or pools using the new logical drive or drives
- Use new pool space to expand existing virtual disks
- Use new pool space or new pools to create new virtual disks

These options give the administrator great flexibility in adding new storage space or effectively expanding existing space. If you add space to an existing pool, the virtual disks created in that pool can be expanded, or new virtual disks can be created to take advantage of the space. Use the procedures described in the previous sections for creating arrays, logical drives, pools, and virtual disks.

When you plan for adding space to your appliance, consider the following:

- Add drives in groups of three or four. Because new drives must be configured as new logical drives, and RAID 5 sets must have at least three members, for best performance add drives in sets of at least three, and preferably seven or more. Sets of 14 reduce the drive space lost to RAID 5 overhead or parity.
- The maximum number of storage units (logical drives) in a pool is eight. If you want to have large pools from which to create virtual disks, it is advantageous to make logical drives as large as possible.
- Each array that you create must have at least one online spare drive. The same online spare drive can be assigned to multiple arrays, but it must be replaced with a new spare if the existing spare is used. The original online spare drive remains a part of the array until the replacement drive is installed.

Bypass Procedure:

To bypass the Configuration Wizard, follow these steps to expand your array:

1. Install the new physical drive or drives.
2. Run the ACU. The utility does not automatically start when new drives are added.
3. Assign the new physical drives to an existing array. You can also create a new array or arrays so that the existing array does not exceed 14 drives. Existing logical drives automatically expand across the physical drives, including newly added ones.
4. Create a new logical drive to use the extra space on the expanded array.

See “Adding Additional Storage Units to the Pool” earlier in this chapter.

Ethernet Teaming Features and Procedures

Compaq Network Teaming and Configuration Utility

The TaskSmart N2400 appliance is equipped with the Compaq Network Teaming and Configuration (CPQTEAM) Utility. The CPQTEAM Utility allows users to configure and monitor Compaq NICs operating under Windows 2000, and provides several options for increasing throughput and fault tolerance when operating under Windows 2000.

- **Fault Tolerance** provides automatic redundancy. If the primary NIC fails, the secondary NIC takes over.
- **Load Balancing** provides the ability to balance transmission across NICs as needed to improve server throughput.

Installing CPQTEAM Utility

Before you can use the CPQTEAM Utility you must first install it. To do this, perform the following tasks.

1. Double click the **CPQTEAM Setup** icon on the desktop.

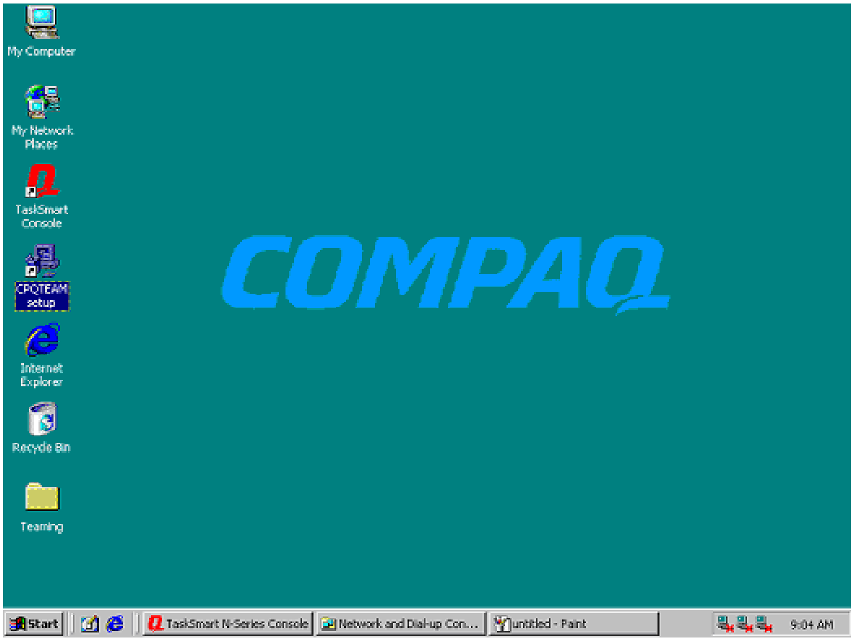
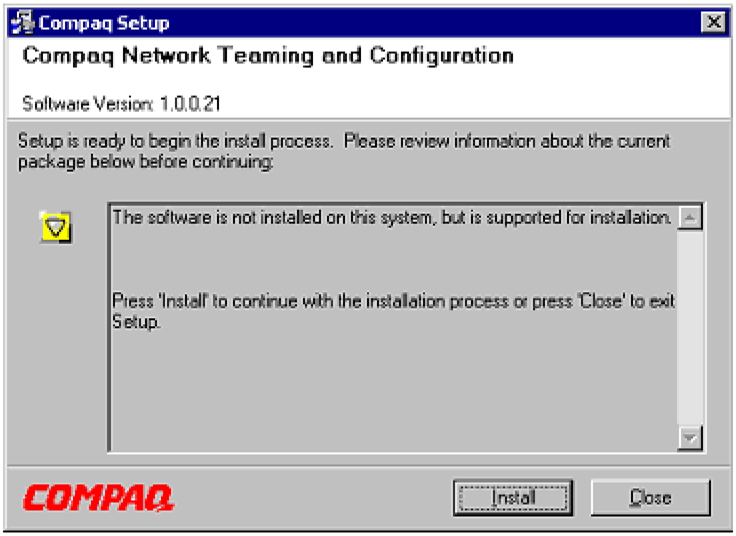


Figure 6-13. Launching CPQTEAM setup

2. When the following message box is displayed, click **Install**.



Software Version: 1.0.0.21

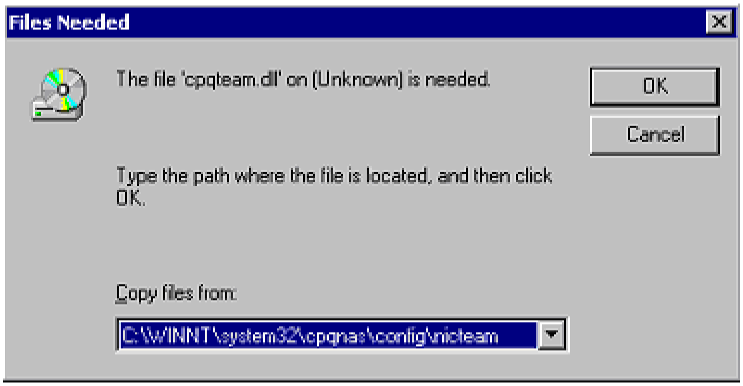
Setup is ready to begin the install process. Please review information about the current package below before continuing:

The software is not installed on this system, but is supported for installation.

Press 'Install' to continue with the installation process or press 'Close' to exit Setup.

Figure 6-14. Installing CPQTEAM

3. Click **OK** when prompted with the following message:



The file 'cpqteam.dll' on (Unknown) is needed.

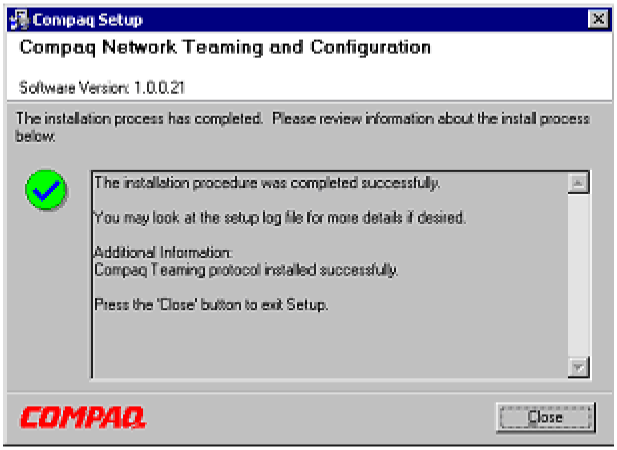
Type the path where the file is located, and then click OK.

Copy files from:

C:\WINNT\system32\cpqnas\config\nicteam

Figure 6-15. Selecting CPQTEAM file path

4. CPQTEAM Utility is installed on your unit. When installation is complete the following screen is displayed. Click **Close.** You are now ready to use the CPQTEAM Utility.



Compaq Setup

Compaq Network Teaming and Configuration

Software Version: 1.0.0.21

The installation process has completed. Please review information about the install process below.

The installation procedure was completed successfully.

You may look at the setup log file for more details if desired.

Additional Information:
Compaq Teaming protocol installed successfully.

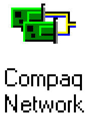
Press the 'Close' button to exit Setup.

Figure 6-16. CPQTEAM installation complete

Opening CPQTEAM Utility

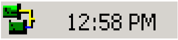
There are two methods to access the CPQTEAM utility:

- From the Windows Control Panel, double-click the **Compaq Network** icon.



-or-

- Double-click the **Tray** icon in the Windows toolbar at the bottom of the Windows 2000 screen.



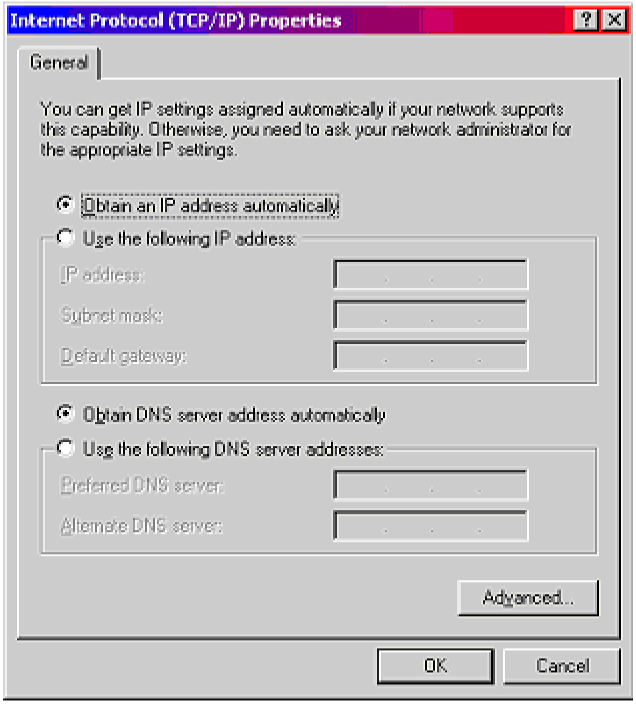
Adding a NIC to a Team

Before a NIC is teamed, verify the following:

- NICs must be on the same network.
- NICs must be DHCP enabled and the DNS server address must be left blank.

> **NOTE:** The Teaming utility becomes unstable if static IPs, Subnets, and DNS addresses are set before Teaming.

The Internet Protocol (TCP/IP) Properties dialog for each NIC must match the screen displayed in Figure 6-17.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

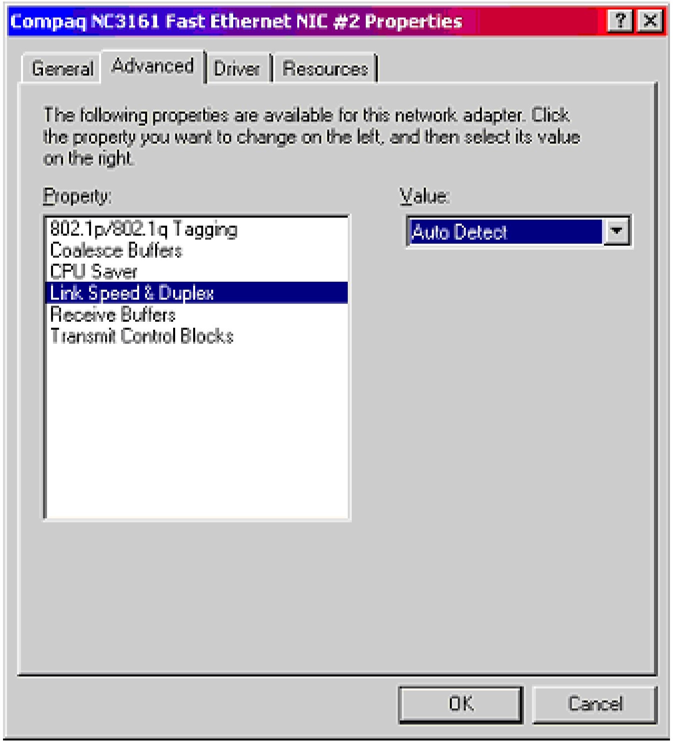
○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

Figure 6-17. Internet Protocol (TCP/IP) Properties dialog box

- NICs duplex and speed settings must be set to default.



The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

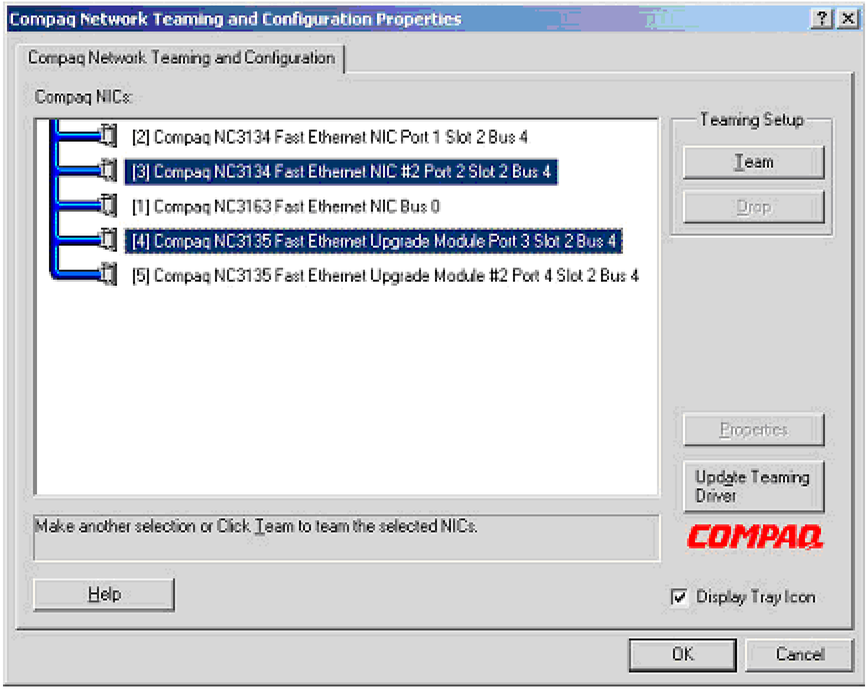
802.1p/802.1q Tagging
Coalesce Buffers
CPU Saver
Link Speed & Duplex
Receive Buffers
Transmit Control Blocks

Value: Auto Detect

Figure 6-18. NIC Properties dialog box

1. Open the CPQTEAM utility.

2. Highlight the NICs that you want to team, and then select **Team.**



[2] Compaq NC3134 Fast Ethernet NIC Port 1 Slot 2 Bus 4
[3] Compaq NC3134 Fast Ethernet NIC #2 Port 2 Slot 2 Bus 4
[1] Compaq NC3163 Fast Ethernet NIC Bus 0
[4] Compaq NC3135 Fast Ethernet Upgrade Module Port 3 Slot 2 Bus 4
[5] Compaq NC3135 Fast Ethernet Upgrade Module #2 Port 4 Slot 2 Bus 4

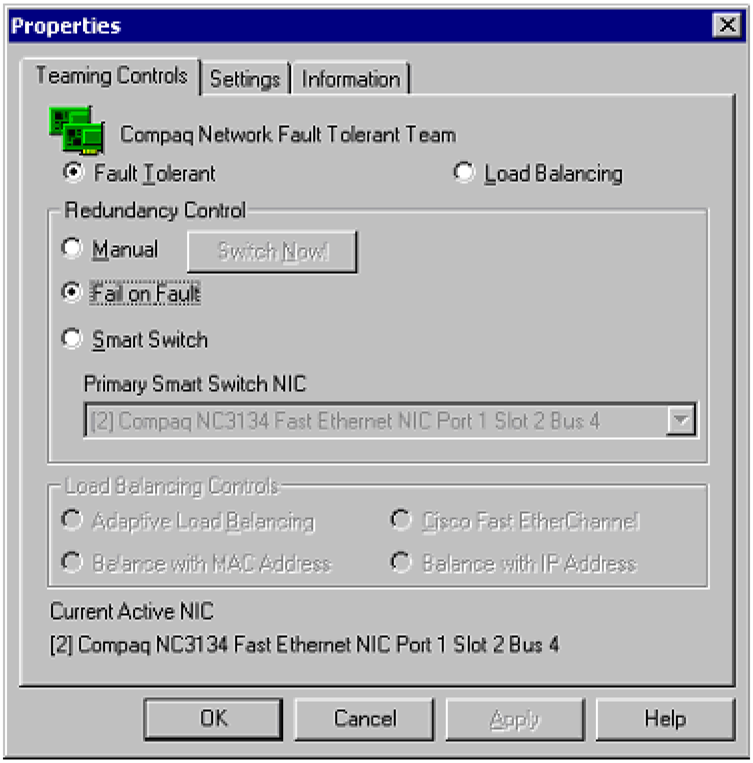
Make another selection or Click Team to team the selected NICs.

Figure 6-19. Compaq Network Teaming and Configuration Properties dialog box

3. Configure the team as desired by choosing either **Fault Tolerance** or **Load Balancing**.

Fault Tolerance

The Fault Tolerance teaming option provides three redundancy control options.



Compaq Network Fault Tolerant Team

● Fault Tolerant ○ Load Balancing

Redundancy Control

○ Manual

● Fail on Fault

○ Smart Switch

Primary Smart Switch NIC

[2] Compaq NC3134 Fast Ethernet NIC Port 1 Slot 2 Bus 4

Load Balancing Controls

○ Adaptive Load Balancing ○ Cisco Fast EtherChannel

○ Balance with MAC Address ○ Balance with IP Address

Current Active NIC

[2] Compaq NC3134 Fast Ethernet NIC Port 1 Slot 2 Bus 4

Figure 6-20. Teaming Controls dialog box, Fault Tolerant option

- **Manual—**This setting lets the user change from a Primary NIC to a Secondary NIC only when the user clicks **Switch Now!**

  NOTE: The Switch Now! Option is disabled until the user selects Manual, and then clicks **Apply**.

- **Fail on Fault—**This setting automatically switches from a Primary NIC to a Secondary NIC when the Primary NIC fails.

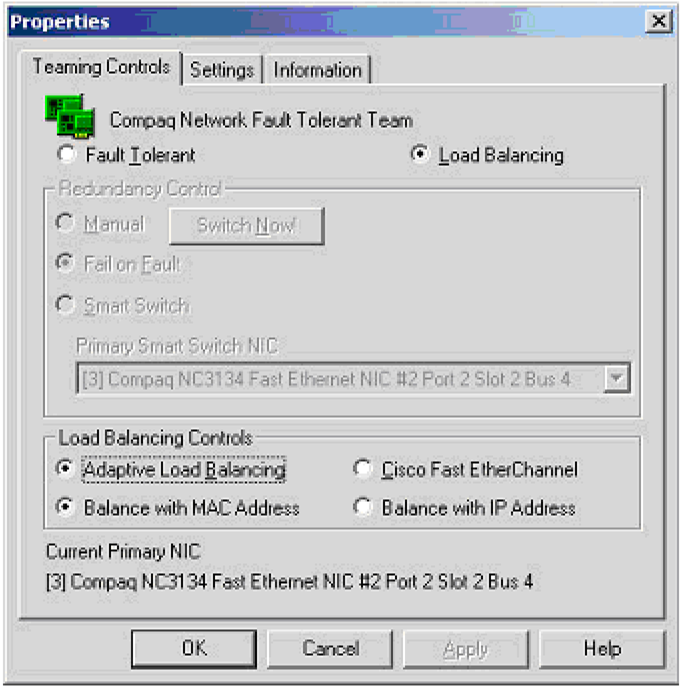
- **Smart Switch—**This setting allows for a member of a team to be selected as the preferred Primary Smart Switch NIC. As long as this NIC is operational, it is always the active NIC. If the NIC fails and it is eventually restored/replaced, it automatically resumes its status as the active NIC.

  NOTE: Because of its functionality, Smart Switch is the recommended choice for Fault Tolerance.

Detailed information about configuring teams for fault tolerance can be found in the Compaq Network Teaming and Configuration Help.

Load Balancing

The Load Balancing teaming option provides four Load Balancing Control options.



Compaq Network Fault Tolerant Team

○ Fault Tolerant ● Load Balancing

Redundancy Control

○ Manual

● Fail on Fault

○ Smart Switch

Primary Smart Switch NIC

[3] Compaq NC3134 Fast Ethernet NIC #2 Port 2 Slot 2 Bus 4

Load Balancing Controls

● Adaptive Load Balancing ○ Cisco Fast EtherChannel

● Balance with MAC Address ○ Balance with IP Address

Current Primary NIC

[3] Compaq NC3134 Fast Ethernet NIC #2 Port 2 Slot 2 Bus 4

Figure 6-21. Load Balancing Control teaming option

- **Adaptive Load Balancing (ALB)—**Creates a team of NICs to increase a server transmission throughput. Works with any 100Base-TX or Gigabit switch. With ALB, you can group NICs into teams to provide a single, virtual NIC with increased transmission bandwidth. To use ALB, you must link at least two teamed Compaq NICs in the server to the same network switch.

- **Cisco Fast EtherChannel (FEC)—**This feature creates a team of NICs to increase transmission and reception throughput. Unlike ALB, Cisco FEC can be configured to increase both transmission and reception channels between the server and switch. For example, a Cisco FEC team containing four Compaq Fast Ethernet NICs configured for full-duplex operation provides an aggregate maximum transmit rate of 400 megabytes per second (Mbps) and an aggregate maximum receive rate of 400 Mbps resulting in a total bandwidth of 800 Mbps.

- **Balance with MAC Address—**This feature allows load-balancing of IP Packets among the teamed NICs using the last four bits of the MAC Address.
- **Balance with IP Address—**This feature allows load-balancing of IP Packets among the teamed NICs using the last four bits of the IP Address.

Load Balancing with MAC or IP Address

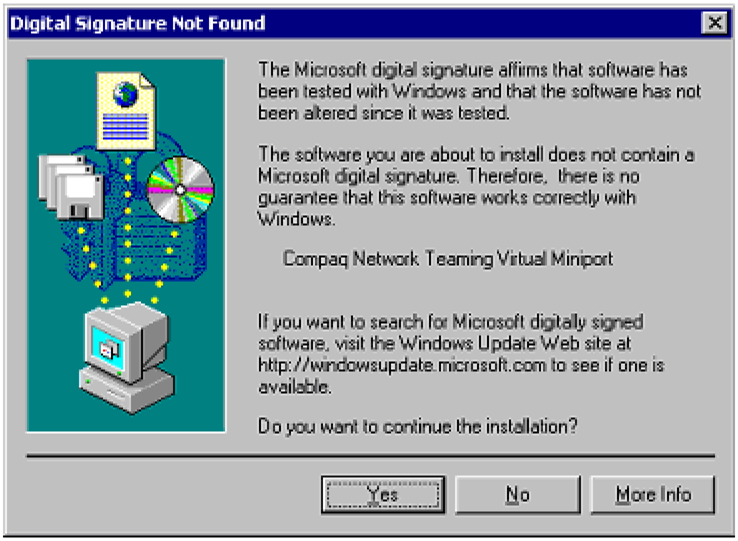
The Windows 2000 Teaming Utility lets you load balance IP Packets among the teamed NICs installed in a server. The primary NIC in the team receives all incoming packets. The choice is available to load balance with the source MAC address (the address transmitted from the workstation) or the source IP address.

Using the last four bits of either source address, the teaming driver algorithm then assigns this source address to the port of one of the NICs in the team. This port is then used to transmit all packets destined for that source address. This configuration the transmission of packets from the server by sharing the packets among all the NICs in the team. If there are four NICs in the team, the packets are received by the primary NIC on the team. The packets are retransmitted through one of the four ports.

Detailed information about these four load-balancing teaming options can be found in the Compaq Network Teaming and Configuration Help.

Licensing

After completing the NIC teaming procedure, warnings similar to the following are displayed.



Digital Signature Not Found

The Microsoft digital signature affirms that software has been tested with Windows and that the software has not been altered since it was tested.

The software you are about to install does not contain a Microsoft digital signature. Therefore, there is no guarantee that this software works correctly with Windows.

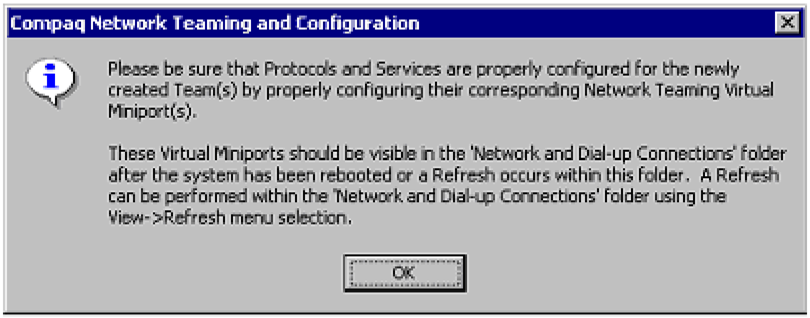
Compaq Network Teaming Virtual Miniport

If you want to search for Microsoft digitally signed software, visit the Windows Update Web site at http://windowsupdate.microsoft.com to see if one is available.

Do you want to continue the installation?

Figure 6-22. License Warning dialog box

When encountering these screens, click **Yes** to continue. The following screen is displayed.



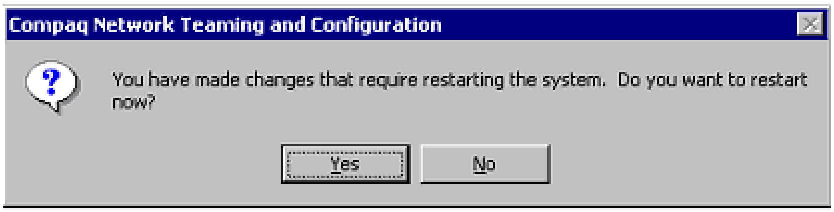
Compaq Network Teaming and Configuration

Please be sure that Protocols and Services are properly configured for the newly created Team(s) by properly configuring their corresponding Network Teaming Virtual Miniport(s).

These Virtual Miniports should be visible in the 'Network and Dial-up Connections' folder after the system has been rebooted or a Refresh occurs within this folder. A Refresh can be performed within the 'Network and Dial-up Connections' folder using the View->Refresh menu selection.

Figure 6-23. Compaq Network Teaming and Configuration dialog box

Click **Yes** to continue, and then you will be asked to reboot the system. At this time close all other open applications, and then click **Yes** to reboot the system.



Compaq Network Teaming and Configuration

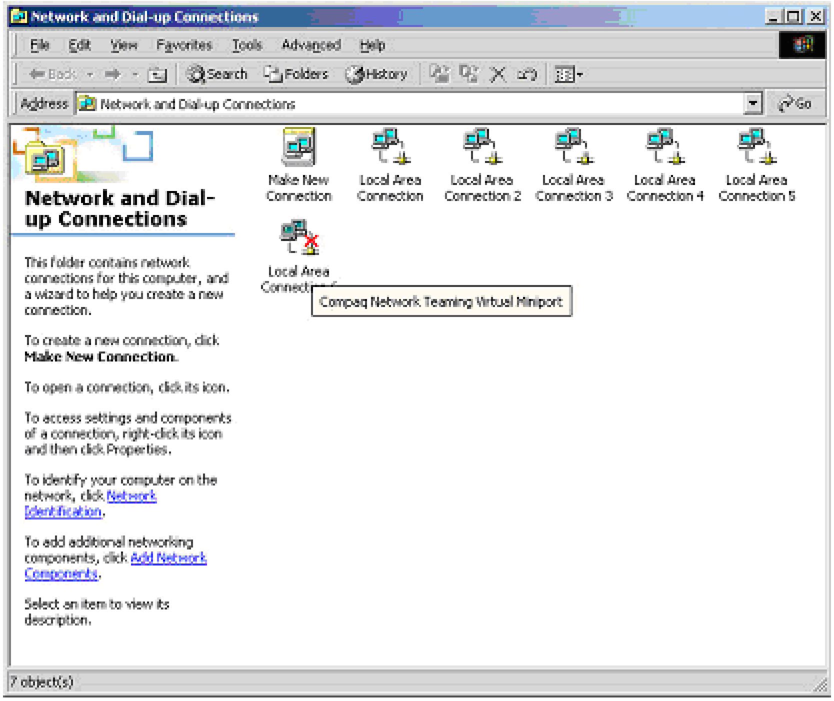
You have made changes that require restarting the system. Do you want to restart now?

Figure 6-24. Compaq Network Teaming and Configuration Restart dialog box

Configuring TCP/IP Protocol on New Team

After the NIC teaming procedure has been completed, a new virtual network adapter is created in the networking properties screen. To access the networking properties, right-click the **My Network Places** icon in the TaskSmart N2400 desktop, and then select **Properties.**

NOTE: The appliance must be restarted before the virtual adapter is created and accessible in the networking properties.


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Make New Connection
Local Area Connection
Local Area Connection 2
Local Area Connection 3
Local Area Connection 4
Local Area Connection 5
Local Area Connecti
Compaq Network Teaming Virtual Miniport
7 object(s)

Network and Dial-up Connections

This folder contains network connections for this computer, and a wizard to help you create a new connection.

To create a new connection, click **Make New Connection**.

To open a connection, click its icon.

To access settings and components of a connection, right-click its icon and then click Properties.

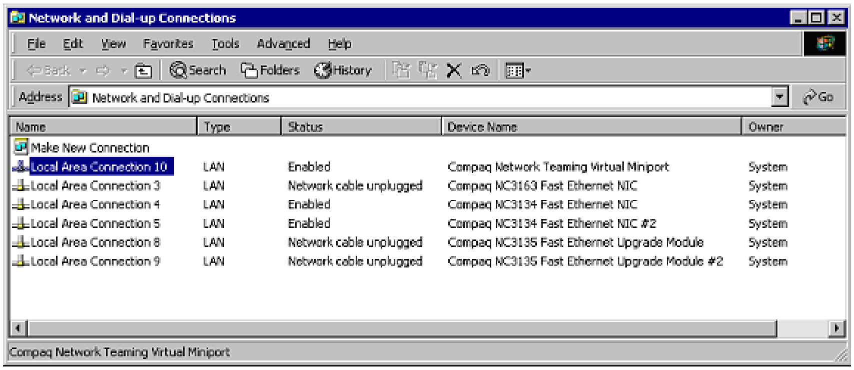
To identify your computer on the network, click Network Identification.

To add additional networking components, click Add Network Components.

Select an item to view its description.

Figure 6-25. Network and Dial-up Connections screen

After the system has powered up, open the Network Properties page, select the **View** tab, and then click on **Details.** The Network Properties page should then look similar to the following.

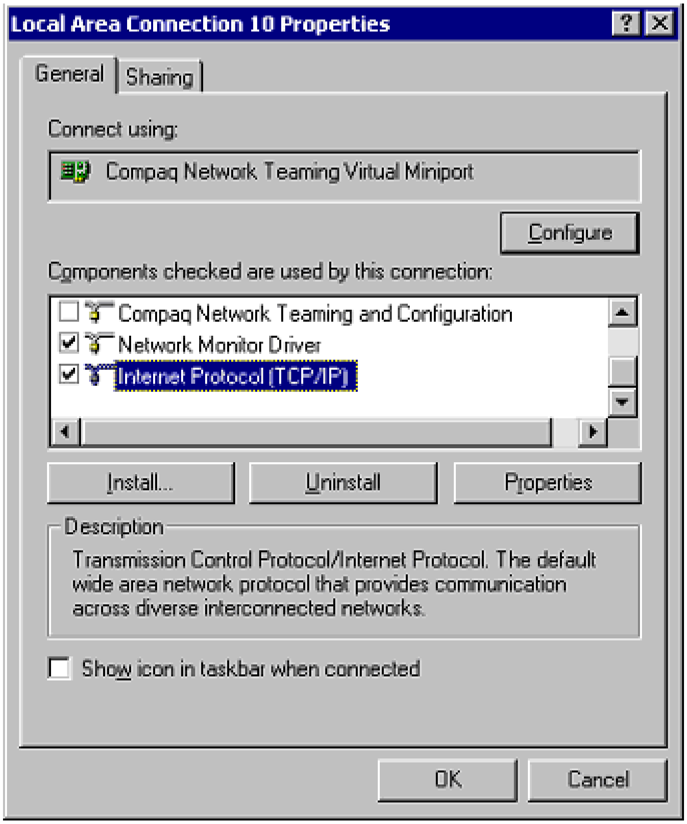


Name	Type	Status	Device Name	Owner
Make New Connection				
Local Area Connection 10	LAN	Enabled	Compaq Network Teaming Virtual Miniport	System
Local Area Connection 3	LAN	Network cable unplugged	Compaq NC3163 Fast Ethernet NIC	System
Local Area Connection 4	LAN	Enabled	Compaq NC3134 Fast Ethernet NIC	System
Local Area Connection 5	LAN	Enabled	Compaq NC3134 Fast Ethernet NIC #2	System
Local Area Connection 8	LAN	Network cable unplugged	Compaq NC3135 Fast Ethernet Upgrade Module	System
Local Area Connection 9	LAN	Network cable unplugged	Compaq NC3135 Fast Ethernet Upgrade Module #2	System

Compaq Network Teaming Virtual Miniport

Figure 6-26. Network Properties dialog box

Right-click on **Compaq Network Teaming Virtual Miniport,** and then select properties. A screen similar to the following is displayed.



Connect using:
Compaq Network Teaming Virtual Miniport

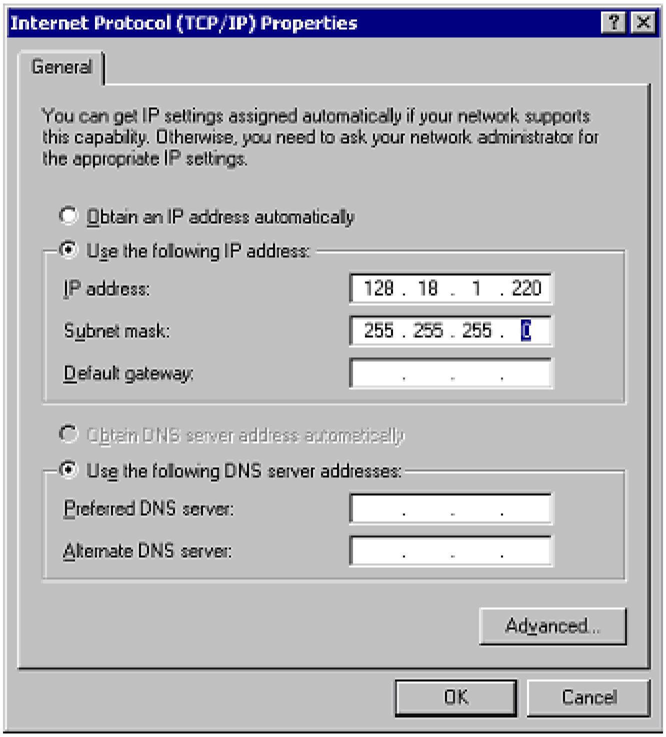
Components checked are used by this connection:
- ☐ Compaq Network Teaming and Configuration
- ☑ Network Monitor Driver
- ☑ Internet Protocol (TCP/IP)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in taskbar when connected

Figure 6-27. Local Area Connection Properties dialog box

Click **Properties** to configure your Teams IP address, Subnet Mask, and DNS address.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 128 . 18 . 1 . 220

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

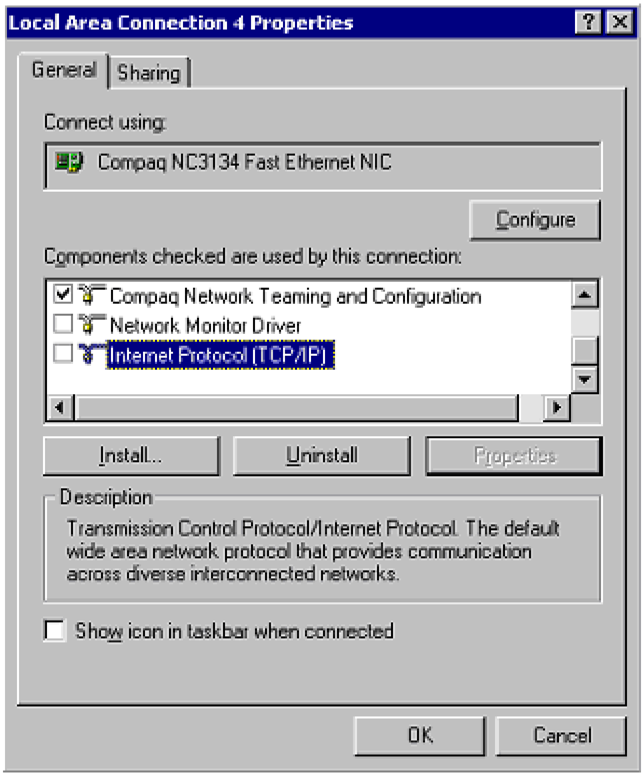
Alternate DNS server: . . .

Figure 6-28. Local Area Connection Internet Protocol Properties dialog box

---

IMPORTANT: When this process is complete, do not modify the TCP/IP Protocols for the individual Ethernet ports that are teamed.

After you have finished configuring the TCP/IP settings, click **OK.** The Ethernet Team should be up and running.



Connect using:

Compaq NC3134 Fast Ethernet NIC

Components checked are used by this connection:

☑ Compaq Network Teaming and Configuration
☐ Network Monitor Driver
☐ Internet Protocol (TCP/IP)

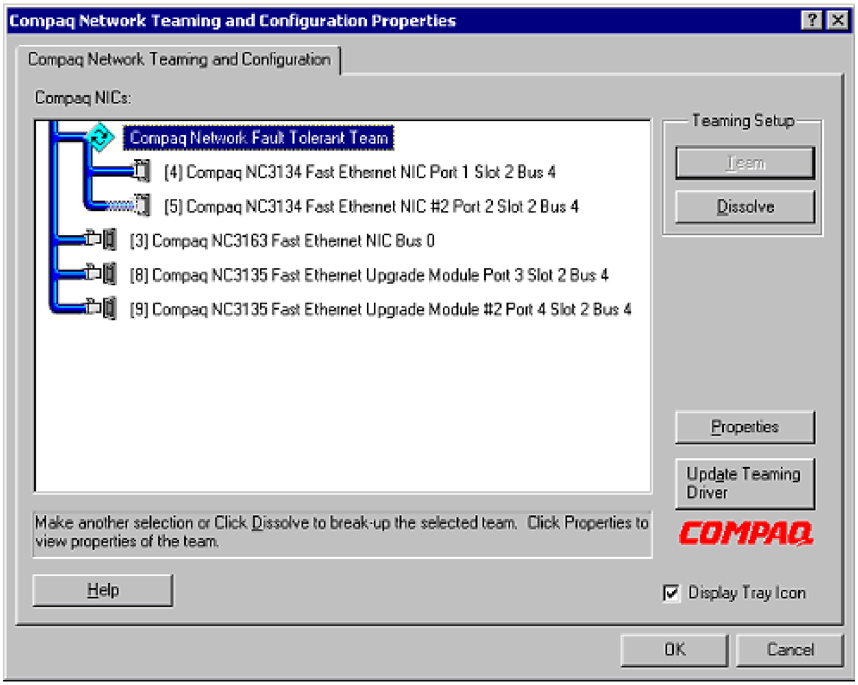
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in taskbar when connected

Figure 6-29. Local Area Connection Properties dialog box

To check the status of the Ethernet Team, launch the CPQTEAM Utility.The following screen is displayed.


Compaq Network Teaming and Configuration Properties
Compaq Network Teaming and Configuration
Teaming Setup
Team
Dissolve
Properties
Update Teaming Driver
COMPAQ
Help
OK
Cancel

Compaq NICs:

- Compaq Network Fault Tolerant Team
  - [4] Compaq NC3134 Fast Ethernet NIC Port 1 Slot 2 Bus 4
  - [5] Compaq NC3134 Fast Ethernet NIC #2 Port 2 Slot 2 Bus 4
- [3] Compaq NC3163 Fast Ethernet NIC Bus 0
- [8] Compaq NC3135 Fast Ethernet Upgrade Module Port 3 Slot 2 Bus 4
- [9] Compaq NC3135 Fast Ethernet Upgrade Module #2 Port 4 Slot 2 Bus 4

Make another selection or Click Dissolve to break-up the selected team. Click Properties to view properties of the team.

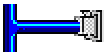
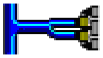
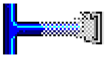
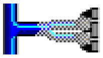
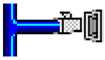
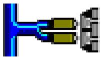
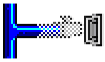
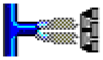
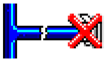
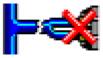
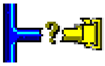
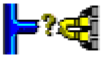
☑ Display Tray Icon

Figure 6-30. Compaq Network Teaming and Configuration Properties dialog box

NIC Teaming Troubleshooting

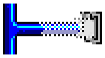
Problems with the NIC teaming feature are diagnosed by the connection icons displayed in the Compaq Network Teaming and Configuration dialog box. The following table lists the error icons for RJ-45 and Gigabit Fibre NICs.

Table 6-4
NIC Teaming Troubleshooting

RJ-45	Gigabit Fibre	Description
		**Active OK—**The NIC is operating properly. The driver is installed in the registry and is loaded. If the NIC is a member of a Team, the NIC is active.
		**Installed inactive—**The NIC is installed and is OK, but is not active
		**Cable fault—**The driver is installed in the registry and is loaded. The broken cable indicator means that the cable is unplugged, loose, broken, or the switch or hub is not operating properly. If this icon is displayed, check all network connection and make sure the hub/switch is working properly. When the connection is restored, this icon will change.
		**Inactive cable fault—**A cable fault has occurred while the NIC was inactive.
		**Hardware failure—**The driver is installed in the registry and is loaded. The driver is reporting a hardware problem with the NIC. This indicates a serious problem. Contact your authorized Compaq service provider.
		**Unknown—**The appliance is unable to communicate with the driver for the installed NIC. The NIC is installed in the registry, but the driver is not. This error occurs when the NIC has been installed but the appliance has not been restarted. If this problem persists after the appliance has been restarted, the driver has not been loaded or the Advanced Network Control Utility is unable to communicate with the driver Note: Only NIC assigned as members of a team are displayed as Unknown. If a teamed NIC is turned off it displays as Unknown.

continued

Table 6-4
NIC Teaming Troubleshooting *continued*

RJ-45	Gigabit Fibre	Description
		**Disabled—**The NIC has been disabled through the Device Manager or NCPA.

For more advanced problems with NIC Teaming refer to the Compaq Network Teaming and Configuration Help section in the CPQTeam Utility.

Using Uninterruptible Power Supplies

Compaq recommends that your TaskSmart N2400 appliance be connected to an uninterruptible power supply (UPS). Companies often have a UPS built into facility power. Most cases require a separate UPS connected to the TaskSmart N2400 appliance.

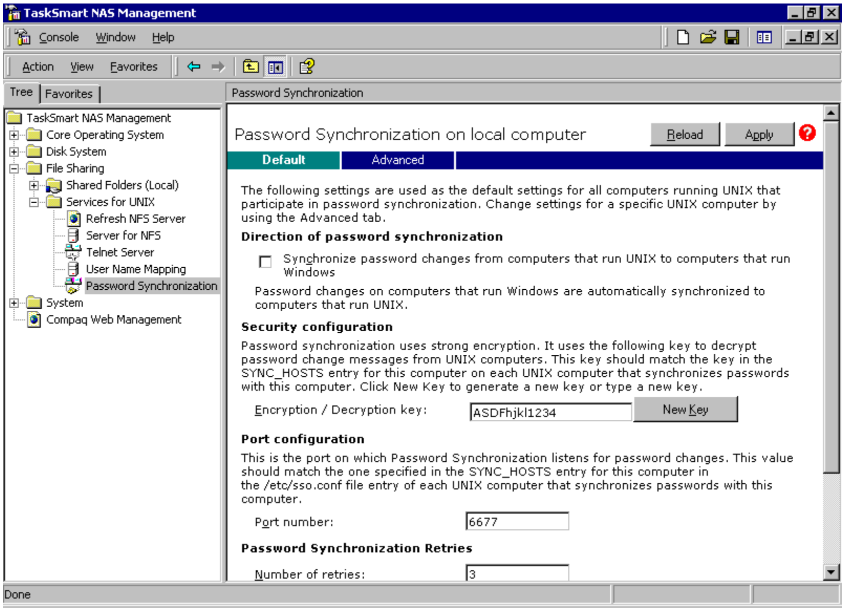
A UPS protects your TaskSmart N2400 appliance from power outages and low-quality power situations, such as dips and spikes. During a power outage, the UPS automatically detects the interruption in power and switches over to an internal battery supply. The battery provides continuous power for a limited amount of time. Power interruptions are often short lived, and the UPS enables the TaskSmart N2400 appliance to continue providing file service until normal power is restored. However, when power fails, the system must be powered down. The UPS supplies a limited amount of power to complete essential tasks and to power down the TaskSmart N2400 appliance, avoiding any loss of data.

The UPS communicates directly with your TaskSmart N2400 appliance through a serial line connection. If the system is properly configured and the serial line connection is established, the UPS notifies the TaskSmart N2400 appliance when power is interrupted. The TaskSmart N2400 appliance then automatically initiates a coordinated power-down. In addition, many UPS products can be remotely controlled and monitored through Compaq Insight Manager.

For detailed information about connecting the UPS to your TaskSmart N2400 appliance, refer to the documentation shipped with your specific UPS product. Compaq offers a broad range of UPS products and can be viewed on the Compaq website. This website provides information about many types of UPS options, as well as a sizing tool with which to choose the proper UPS for your TaskSmart N2400 appliance.

Password Synchronization

Password synchronization is an optional service that automatically synchronizes Windows Powered OS passwords with UNIX passwords across multiple machines or environments. Administrators and users have little trouble remembering or managing passwords when one machine is involved. Tracking user names and passwords across multiple account databases can be problematic.



Password Synchronization on local computer

The following settings are used as the default settings for all computers running UNIX that participate in password synchronization. Change settings for a specific UNIX computer by using the Advanced tab.

Direction of password synchronization

☐ Synchronize password changes from computers that run UNIX to computers that run Windows

Password changes on computers that run Windows are automatically synchronized to computers that run UNIX.

Security configuration

Password synchronization uses strong encryption. It uses the following key to decrypt password change messages from UNIX computers. This key should match the key in the SYNC_HOSTS entry for this computer on each UNIX computer that synchronizes passwords with this computer. Click New Key to generate a new key or type a new key.

Encryption / Decryption key: ASDFhjkl1234

Port configuration

This is the port on which Password Synchronization listens for password changes. This value should match the one specified in the SYNC_HOSTS entry for this computer in the /etc/sso.conf file entry of each UNIX computer that synchronizes passwords with this computer.

Port number: 6677

Password Synchronization Retries

Number of retries: 3

Figure 6-31. SFU Password Synchronization dialog box

Password synchronization ensures that the machines contain the identical, most current user password database. When the user or administrator changes a password, the new password is updated across all target machines.

Without password synchronization, the user could have different passwords on different machines. If the administrator or user changed the password, the change would affect only that single machine. Such a scenario can quickly become an administrative nightmare.

Implementation

The password synchronization service is a service residing on the NFS server. The service does not have to be on the same server as the NFS server, but the service is included on each TaskSmart N2400 appliance. The password synchronization service detects updates on the Windows NT side and transmits the changes to the target UNIX machines, as specified in the service configuration. The service also checks for incoming changes from the UNIX side if that direction of propagation is enabled.

Requirements

Password synchronization is bidirectional. It works from NT to UNIX and from UNIX to NT. The work environment **must** meet the following criteria for the password synchronization service to function:

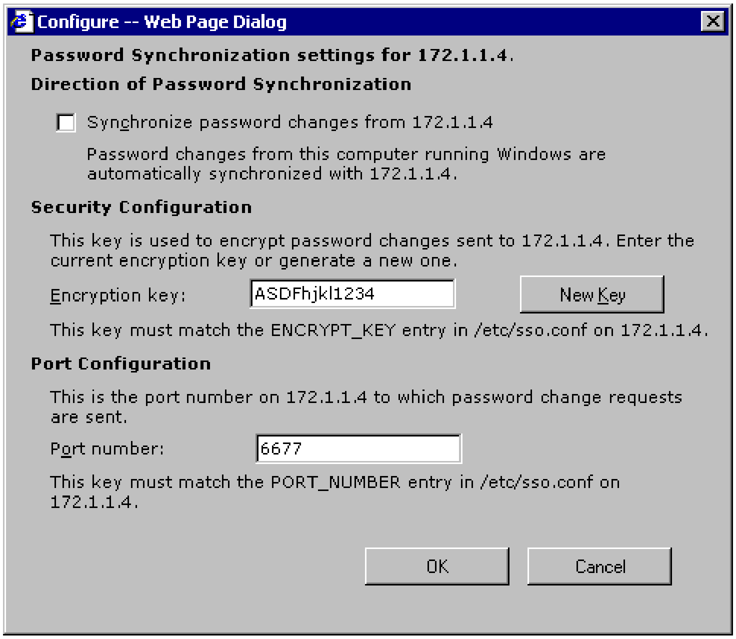
- The password policies must be the same on NT and UNIX.
- User and group names must match exactly in spelling. No “advanced mapping” component exists to correct for any mistakes or differences.
- The UNIX system must be using CRYPT to encrypt its password database. If the UNIX machine is using anything else, such as MD5, the password synchronization service does not work.
- The password synchronization service must be installed on the primary and backup domain controllers. Click the **Advanced** button to select settings other than default.

Password Synchronization—Advanced Settings

To configure advanced settings for password synchronization, use the following procedure:

1. Type the name or IP address of the UNIX computer in the Computer Name box.
2. Click **Add,** and then click **Configure.** The password synchronization settings dialog box for the specific computer is displayed.

This dialog box allows the user to perform steps such as supplying new encryption keys or changing password synchronization port numbers.



Password Synchronization settings for 172.1.1.4.

Direction of Password Synchronization

☐ Synchronize password changes from 172.1.1.4

Password changes from this computer running Windows are automatically synchronized with 172.1.1.4.

Security Configuration

This key is used to encrypt password changes sent to 172.1.1.4. Enter the current encryption key or generate a new one.

Encryption key: ASDFhjkl1234

This key must match the ENCRYPT_KEY entry in /etc/sso.conf on 172.1.1.4.

Port Configuration

This is the port number on 172.1.1.4 to which password change requests are sent.

Port number: 6677

This key must match the PORT_NUMBER entry in /etc/sso.conf on 172.1.1.4.

Figure 6-32. SFU Password Synchronization dialog box, advanced settings

Installation Procedure

The password synchronization service must be installed on all primary domain controllers (PDC) and backup domain controllers (BDC) located in a domain, to support the service. PDCs are the system that contains the primary copy of the user passwords.

You do not need core SFU components to install the service on a domain controller. Instead, you can install password synchronization by itself.

NOTE: This procedure does not install SFU.

To install password synchronization on a domain controller:

1. Locate the sfucustom.msi file located in the SFU directory of the N2400.
2. On the domain controller where the service is being installed, do the following:

   Use Windows Explorer:

   a. Open the shared directory containing sfucustom.msi.
   b. Double-click the file to open it. Windows Installer launches.

   NOTE: If the domain controller used does not have Windows Installer installed, locate the file InstMSI.exe in the SFU directory and launch it. After this installation, the Windows Installer program starts when opening sfucustom.msi

   c. Click **Next** when the Welcome to Windows Services for Unix screen is displayed.
   d. Type in the User name and Organization, and then click **Next.**
   e. Accept the license agreement, and then click **Next.**
   f. Select **Custom Installation**, and then click **Next.**
   g. Add the *Will be installed on local hard drive* option for Password Synchronization.
   h. Select the installation directory, and then click **Next.**
   i. Click **Finish** when install is complete.

   NOTE: Windows Installer restarts the computer while installing password synchronization. Before installing password synchronization, be sure to close all applications and notify users connected that the server is powering down.

Password Synchronization—Default

Use **Default** to select password synchronization settings. Select different settings for each UNIX host in the Hosts tab.

- **Direction of Password Synchronization—**This option must remain unchecked. Password changes on Windows NT/2000 are always propagated to UNIX computers. Synchronize password changes from UNIX machines to Windows NT/2000.
- **Security configuration—**Password synchronization uses strong encryption for propagating passwords.
- **Encryption key—**Password synchronization comes with a default Encryption Key (displayed). Enter an encryption key of your own, regenerate the key, or do both.
- **Port configuration—**This port is where the password synchronization service checks for password changes. UNIX machines must be configured to use the defined port number.
- **Password Sync Retries—**Select Password Sync Retries to determine how Password Synchronization failures are handled.
- **Logging—**Significant password synchronization events are logged to the event viewer. Select the option to allow or deny extensive logging.

Appendix A

Backup Utility Management

The Compaq TaskSmart N2400 appliance is a complete, engineered solution for network attached storage (NAS). Using tuned hardware and reliable operating system and software components in an integrated and tested package, the TaskSmart N2400 appliance enables companies to begin realizing the benefits of NAS.

As a source and destination for departmental, workgroup, or even enterprise data, the TaskSmart N2400 appliance becomes an integral part of company computing environments. Therefore, efficient backup and reliable restore capabilities are a priority.

It is important to configure a reliable and efficient backup solution before storing important data on the TaskSmart N2400 appliance. This appendix provides pointers for setting up and maintaining reliable backups.

Sizing Tools

There are many factors to consider when choosing a backup solution for your particular environment. These factors include performance, capacity, reliability, automation, and cost issues. If you have not already made decisions in these areas, Compaq provides some useful tools that make this process easier. Information about backup products is available on the Compaq website:

http://www.compaq.com

Specific references for the following can be found on the Compaq website:

http://www.compaq.com/products/storageworks/

- Direct connection sizing tool
- Enterprise Backup Solutions backup sizing white paper
- Fibre connection sizing tool

Developing a Backup Solution

There are three main considerations when developing a backup solution:

- Types of tape solutions
- Tape device connection methods:
  - SCSI
  - Fibre Channel
- Backup software vendors

In many departmental and workgroup situations, it is common to connect a tape backup device directly to the appliance, providing the server with exclusive use of the tape device. Due to common usage in the industry and excellent performance and capacity, several tape solutions are recommended by Compaq later in this appendix for use with the TaskSmart N2400 appliance.

In enterprise situations, it is typical for multiple servers to share a large tape library device through a storage area network (SAN). Depending on your desire to share a tape library and your number of servers, a new SAN for backups can be set up. Another option is to extend an existing SAN to include your TaskSmart N2400 appliance.

Types of Tape Solutions

Compaq recommends several tape solutions for use with the TaskSmart N2400 appliance. The solutions in the following list are based on the DLT 35/70 tape drive:

IMPORTANT: You must verify that your specific backup software solution is compatible with these tape device solutions.

- Compaq standalone DLT 35/70
- Compaq DLT Tape Array
- Compaq DLT MiniLibrary TL891/892
- Compaq DLT Library TL895
- Compaq AIT Library SSL2020TL

Tape Device Connection Methods

If you have chosen to connect a tape device to your TaskSmart N2400 appliance, the next step is to select the tape device and backup software. The most direct way to back up your TaskSmart N2400 appliance is to connect a tape library, tape array, or one or more stand-alone tape drives to your appliance using a direct SCSI connection.

SCSI Direct Connect Environments

To implement a SCSI-connected solution, you must determine which tape device that you are connecting. Single-ended (SE) SCSI devices can be connected directly to the integrated SCSI connector on the TaskSmart N2400 appliance. SE devices include stand-alone tape drives, Compaq DLT tape arrays, and some small tape autochangers. Check the tape device product documentation to verify that an SE connection exists. The integrated SE SCSI connector supports up to two DLT 7000 (35/70-GB) tape drives on a single SCSI bus.

Other tape devices use High Voltage Differential (HVD) or Low Voltage Differential (LVD) connections. Typical HVD or LVD tape devices include the Compaq DLT TL891 MiniLibrary, the Compaq TL895 Library, and other autochangers. To use these devices, an optional SCSI tape controller must be used in PCI slot 4 in the server. The optional HVD or LVD controller has two SCSI buses, each capable of supporting up to two DLT 7000 (35/70-GB) devices, for a total of four tape drive devices.

Before purchasing a tape device, make sure that the backup software supports it. Most backup software supports all types of backup devices, but you should confirm your specific choice by consulting the software vendor website. Vendors usually post a hardware compatibility guide for each version of the backup software application.

Fibre-Channel Environments

If your company is already sharing tape libraries, or planning this approach, you need to ascertain which of the following Fibre Channel environments is being used:

- Fibre-Channel Arbitrated Loop (FC-AL)
- Switched Fibre Channel

Fibre Channel loop environments connect servers, such as the TaskSmart N2400 appliance, to backup devices using a Fibre Channel hub and a Fibre-Channel-to-SCSI bridge, called a Fibre Channel tape controller. The Fibre Channel loop host bus adapter (HBA) controller is inserted into PCI slot 4 in the server, and a fiber link connects the controller to the fiber hub. Other servers can also be connected to the hub in the same way. A separate fiber link connects the hub to the Fibre Channel tape controller. Finally, a differential or SE SCSI cable connects the tape controller to the actual SCSI tape device or devices.

Fibre Channel switched environments are similar to loop environments, except that a different HBA controller is used in PCI slot 4, and a fibre switch replaces the fibre hub used in the loop environments. Switched environments can be made more reliable than loop environments.

As with the SCSI-connected environments, verify that your chosen backup software vendor supports the specific hardware environment that you plan to operate.

Backup Software Vendors

You can choose a backup software vendor for the TaskSmart N2400 appliance. If you are already utilizing backup software on other services, use the same software to reduce the complexity and setup time of your backup solution.

The TaskSmart N2400 appliance also contains an integrated backup solution that can be used for basic backup functionality. This solution does not have all the functionality and features offered by third-party solutions. Compaq recommends that you select and purchase a third-party backup solution that meets your needs. These needs include such capabilities as tape hardware support and connection method support.

Important capabilities to look for in backup software include the following:

- Autochanger support
- Tape media management database
- File history database with extensive search capabilities
- Ability to define backup groups and schedules
- Ability to take advantage of multiple tape devices concurrently, to reduce backup window
- Options to enable backup of open and locked files
- Options to back up system state and system databases
- Options to interact with software from a remote console application
- Capabilities to analyze, summarize, and report status automatically

Backup Best Practices

The following are general recommendations for performing backups. Keep your company-specific needs and environment in mind when implementing these suggestions.

The Case for Regular and Reliable Backups

The TaskSmart N2400 appliance has a range of high-availability features, including:

- RAID 5 for the data drives
- RAID 1 (mirroring) for the operating system drives
- Snapshots

In addition to these features, regularly scheduled backups to removable media are crucial in safeguarding your data against accidental loss, intentional tampering, or hardware failures.

It is recommended that you configure data disks in RAID 5 arrays. This configuration makes data loss due to disk failure unlikely. Two drives in the same array would have to fail at the same time for data loss to occur. Nevertheless, it can happen, and backups prevent an inconvenience from becoming a tragedy.

Archive Your Server Setup Information

Server setup information includes:

- Server name
- IP addresses
- Gateways
- DNS servers
- NIS servers
- User mapping database
- Drive array

- Logical disk information
- SANworks Virtual Replicator (SWVR):
  - ☐ Pool names
  - ☐ Sizes
  - ☐ Member logical drives
  - ☐ Virtual disk names and sizes

This information greatly increases your ability to quickly and accurately recover from catastrophic failures such as:

- Fires
- Weather disasters
- Theft
- Complete hardware failures

Backup Schedules

Automatic backup schedules are necessary and are dependent on the specific needs of your company. An automatic periodic backup is much more reliable than occasional backups, which often occur when someone remembers to execute them.

Full backups on a weekly or bi-weekly basis are necessary. Depending on the rate that your data changes, and the capacity and performance of your backup devices, adjust the backup schedule to fit your company environment.

If your backup devices do not have sufficient capacity for a full backup, distribute the backups so that they occur throughout the backup cycle. For example, instead of doing a full backup of disks C:, X:, Y:, and Z: all on Friday, you might back up C: on Monday, X: on Tuesday, Y: on Wednesday, and Z: on Thursday. Schedule incremental/differential backups accordingly.

> **NOTE:** The suggested scenarios for backup times are based on a hypothetical company situation.

Taking Advantage of Multiple Backup Devices

To take advantage of multiple backup devices, the server must be configured correctly. For example, if your TaskSmart N2400 appliance has 500 GB of disk space and is contained in a single virtual disk, it is not beneficial to have more than a single tape device.

If you can configure several backup groups to consist of the various directory trees at the root of the virtual disk, more than one tape device can work. It is better to have multiple virtual disks so that each backup operation has a tape device. Using this method, the virtual disks are backed up in parallel taking less time.

Media Rotation

Most backup software solutions are equipped to label and track media usage accurately. Take advantage of these capabilities to maintain different media pools for full backups and incremental/differential backups, as well as archive media. The retention time on each of these types of backup is different. For example, using differential backups on the same tape for full backups causes the tape space to be wasted, after the retention time for the differential data has passed. Keep separate pools to avoid this problem.

Offsite Storage

Be sure to set up a regular process for shipping important long-term media offsite for safekeeping. This plan ensures that you can recover your data in case of a complete facility destruction at the site of the TaskSmart N2400 appliance.

Readiness Testing

Completing regular backups is good. However, the ability to recover and restore data is the important issue. It is important to regularly test the recoverability of random files or directories to ensure that your backup solution is working as designed.

Disaster Recovery

Disasters that cause the loss of your entire server or server operating system drives require a complete restoration of the server. The specific procedure for recovering from a disaster depends on your backup software and the optional disaster recovery modules that you may have installed. In general, it is necessary to complete the following functions to fully recover from a disaster:

- Use the QuickRestore process to reinstall the TaskSmart system image.
- If you made changes to the factory drive array default configuration, configure your arrays, logical drives, pools, and virtual disks as they were at the time of the disaster.
- Reinstall the backup application.
- Add the TaskSmart N2400 appliance into the appropriate domain.
- Re-establish user accounts if the TaskSmart is a part of a workgroup.

  If the files were retained, re-establish user rights to drives, files, and directories.

  NOTE: Being a part of a domain negates this requirement.
- Recover the backup application file and media history databases.
- Recover your data from your backup application.
- Recover the system state.

Appendix B

RAID Levels

Distributed Data Guarding

Distributed data guarding, also called RAID 5, stores parity data across all the drives in the array. Spreading the parity across all the drives allows more simultaneous read operations and higher performance than data guarding (RAID 4). If one drive fails, the controller uses the parity data and the data on the remaining drives to reconstruct data from the failed drive. RAID 5 allows the system to continue operating with reduced performance until you replace the failed drive. If more than one drive fails, RAID 5 also fails, and all data in the array is lost.

Distributed data guarding requires an array with a minimum of three physical drives. In an array containing three physical drives, distributed data guarding uses only 33 percent of the total logical drive storage capacity for fault tolerance; a 14-drive configuration uses only seven percent.

> **NOTE:** Given the reliability of a particular generation of hard drive technology, the probability of an array experiencing a drive failure increases with the number of drives in an array. Compaq recommends the number of drives in an array be limited to 14.

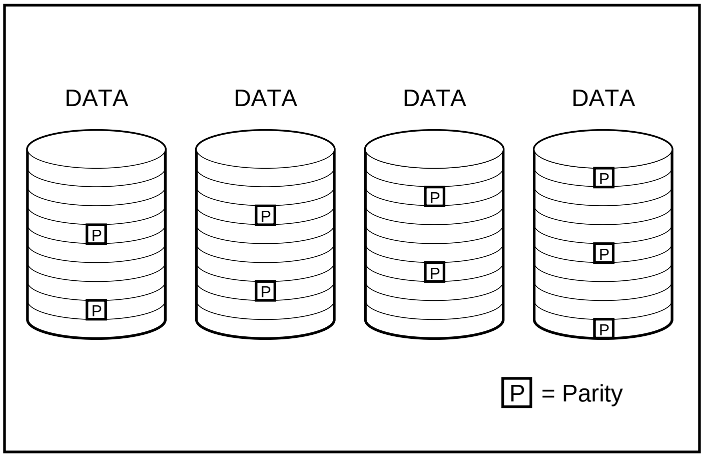


Figure B-1. Distributed data guarding, RAID 5, distributes redundant data (Parity) throughout physical drives

Drive Mirroring

The operating system drives are protected by RAID 1, or drive mirroring. RAID 1 is the highest-performance fault-tolerance method. RAID 1 is the only method for fault-tolerance protection if only two drives are installed or selected for an array. Drive mirroring creates fault tolerance because both drives are exact copies of each other. If one drive fails, the other immediately takes over. RAID 1 is an expensive fault-tolerance method because 50 percent of the drive capacity is used to store the backup copy.

IMPORTANT: The configuration that Compaq supports uses RAID 1 on the system drives in a two-drive RAID set.

RAID 1 requires an even number of drives. To improve performance in configurations with more than two drives, the data is striped across the drives. This is referred to as RAID 0+1, or RAID 10.

If a drive fails, the mirror drive provides a backup copy of the files, and normal system operations are not interrupted. For example, consider the following scenario:

When eight drives are used in a RAID 0+1 configuration, each RAID 0 subarray consists of four drives. Each of the four drive subarrays is a mirror of the other four drive subarrays.

If there is a single drive failure, the data remains intact. A single drive failure causes an individual subarray to stop working. RAID 0 is not fault tolerant. One drive failure results in the loss of the affected array. The mirrored RAID 0 subarray is an exact copy, allowing the system to continue to work.

However, if both subarrays fail, all data is lost. The dual failure causes the entire RAID 0 + 1 array and Array Configuration Utility (ACU) to fail. If the failure is on the operating system drive, the system stops completely.

IMPORTANT: If two drives being mirrored to each other both fail, data loss occurs.

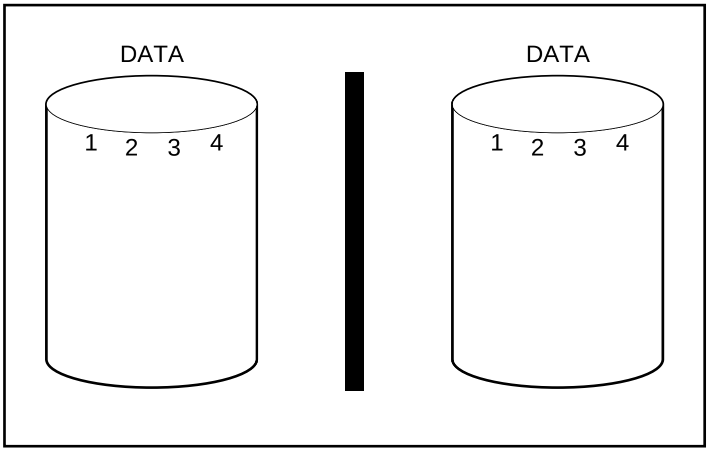


Figure B-2. Drive mirroring, RAID 1

Use ACU to configure your array controller and add additional drives to an existing configuration. ACU can also completely reconfigure your drive array. Reconfiguring your drive array is considered a “data destructive” operation. ACU warns you about destructive operations before it performs them.

The ACU graphical configuration utility is run from the operating system. Use ACU to create RAID array sets and logical drives from the physical drives installed in the storage enclosure. The ACU graphical configuration utility allows the user to set RAID type and other important settings that can affect the performance and fault-tolerant capabilities of the TaskSmart N2400 appliance.

With the TaskSmart N2400 appliance, you can increase storage capacity without taking the server offline. Innovative features allow you to change your array configuration as storage needs grow.

Appendix C

Troubleshooting

This appendix provides troubleshooting information for the TaskSmart N2400 appliance. The following sections cover troubleshooting for common hardware, as well as troubleshooting for hardware and software specific to the appliance:

- Initial Troubleshooting Checklist
- Hard Drive Problems
- SCSI Device Problems
- TaskSmart N2400 Server Troubleshooting
- Software and Firmware Diagnostic Tools
- SFU Troubleshooting
- Stopping and Starting NFS File Service
- NIC Troubleshooting
- Remote Insight Lights-Out Edition Board Troubleshooting
- QuickRestore
- Miscellaneous Troubleshooting

Initial Troubleshooting Checklist

Check the following before attempting other solutions or calling for service:

- Is the TaskSmart N2400 appliance connected to a working power outlet?
- Is the TaskSmart N2400 appliance powered up and the power light illuminated?
- Are all cables properly connected and seated?

For assistance with hardware problems not addressed in this appendix, refer to the “Getting Help” section in the introductory chapter of this guide for Compaq technical support contact information.

Hard Drive Problems

Use this section to troubleshoot hard drive problems. For more troubleshooting tips, also see “SCSI Device Problems” later in this appendix.

IMPORTANT: If the hard drive Fault LED is on, follow the proper troubleshooting procedures, find the cause of the problem and fix it. One common mistake with failed hot-plug drives in a fault tolerant array is hot-plugging (removing the drive for a few seconds and reseating the same drive) without fixing the cause. Hot-plugging often causes the Fault LED to turn off, but does not solve the problem that caused it to light initially. Usually the drive needs replacing, but in some situations a problem could exist with the drive cage, the SCSI cable, or the controller.

Each hot-plug SCSI hard drive has three LEDs located on the front of the drive. The LEDs provide activity, online, and fault status for each corresponding drive when configured as a part of an array and connected to a powered-up Smart Array Controller. The LED behavior can vary, depending on the status of other drives in the array. Refer to your server-specific user documentation for specific information about drive statuses.

WARNING: To reduce the risk of personal injury and damage to the equipment, read the “Hot-Plug Hard Drive Replacement Guidelines” in the next section of this appendix before removing a hard drive.

For more information on individual drive specifications, refer to your server-specific user documentation, the maintenance and service guide, the drive documentation, and the array controller documentation.

Table C-1
Hard Drive Problems

Symptom	Possible Problem	Possible Solution
Hard drive fails, and your system completes Power-On Self-Test (POST).	Hard drive failed.	Replace hard drive.
	Drive is not supported.	Replace with a hard drive supported by the TaskSmart N2400 appliance.
	A SCSI cable failed.	Check the connectors on both ends of all SCSI cables in the configuration. The cables may be damaged.
Hard drive is not recognized by server.	Hard drive connection problem occurred.	Check the LEDs on the hard drive. See “Hard Drive LED Indicators” in Chapter 4, “Integrating UNIX into Windows NT,” of this administration guide. Try removing and replacing the hard drive. If you remove any hard drives, label the drive and its position, and make sure that you install it in the original position.
	Driver problem occurred.	Install correct controller drivers.
The server response time is slower than usual.	Virtual disk is full.	Has the virtual disk become full? As a rule of thumb, virtual disks should maintain 15% free disk space.

continued

Table C-1
Hard Drive Problems *continued*

Symptom	Possible Problem	Possible Solution
No hard drives are recognized.	Power problem is occurring.	Check power to the storage cabinet.
The new hard drive is not recognized.	Drive bay is bad.	Try another bay.
	Hard drive is not supported.	Refer to your hard drive documentation to verify that the hard drive is supported.
	Hard drive failed.	Replace the hard drive.
	Hard drive sizes are incorrectly reported.	Run the Array Configuration Utility.

⚠ **WARNING:** To reduce the risk of personal injury and damage to the equipment, read the "Hot-Plug Hard Drive Replacement Guidelines" in the following section before removing a hard drive.

Hot-Plug Drive Replacement Guidelines

You can hot-plug a drive during normal activity. Be aware, however, that hot-plugging a drive affects system performance and fault tolerance.

NOTE: Depending upon your configuration, both a hard drive failure and the subsequent rebuild process can cause storage subsystem performance degradation. For example, the replacement of a single drive on an array with 16 drives has less impact than a replacement on an array with three drives.

When a drive is hot-plugged, the drive subsystem may no longer be fault tolerant although the system is functionally operational.

△ **CAUTION:** Fault tolerance is lost until the removed hard drive is subsequently replaced and the rebuild operation is completed (this process takes several hours, even if the system is not busy while the rebuild is in progress). If another drive in the array incurs an error during the period when fault tolerance is unavailable, it is possible to cause a fatal system error due to a data error. If another drive fails during this period, the entire contents of the array are lost.

IMPORTANT: It is recommended that a hard drive replacement be performed during low activity periods. In addition, a current valid backup must be available for the logical drives in the array of the drive being replaced, even if drive replacement is being made during server downtime.

Unsafe Hot-Plug Drive Replacement Precautions

Be aware of the following Compaq guidelines cautioning unsafe hot-plug replacement.

- Do not remove a degraded drive if any other member of the array is offline (the online LED is off). No other drive in the array can be hot-plugged without data loss. The possible exception to this might be the utilization of RAID 0+1 as a fault-tolerant form. In this case, drives are mirrored in pairs. More than one drive can fail and be replaced as long as the drive or drives that they are mirroring are online.
- Refer to your Smart Array Controller user guide for information on fault-tolerance options.
- Do not remove a degraded drive if any member of an array is missing (previously removed and not yet replaced).
- Do not remove a degraded drive if any member of an array is being rebuilt, unless the drive being rebuilt has been configured as an online spare. The online LED for the drive flashes, indicating that a replaced drive is being rebuilt from data stored on the other drives.

  NOTE: An online spare does not activate and start rebuilding after a predictive failure alert, because the degraded drive is still online. The online spare activates only after a drive in the array has failed.

- Do not replace multiple degraded drives at the same time (for example, when the system is off), because the fault tolerance may be compromised. When a drive is replaced, the controller uses data from the other drives in the array to reconstruct data on the replacement drive. If more than one drive is removed, a complete data set is not available to reconstruct data on the replacement drive or drives and permanent data loss can occur.

CAUTION: Do not power down a storage enclosure when the server containing the Smart Array Controller is powered up. Also, do not power up the server before powering up the storage enclosure. If these ordering rules are not followed, the Smart Array Controller can mark the drives in the storage enclosure as “failed,” which can result in permanent data loss.

Predictive Failure Alert

The predictive failure alert is a powerful problem-prevention tool that warns you when the system has determined a drive failure is imminent. This alert allows you to proactively schedule downtime for maintenance and not interrupt critical business operations that rely on your servers. In addition, with hot-pluggable drives connected to Compaq Smart Array Controllers, you can remove and replace one or several drives within a server while the system is online, which minimizes the interruption of the network, server downtime, and data loss. Refer to your Compaq Insight Manager and Compaq Management Agents for Servers documentation (found on the Compaq Management CD) for instructions on implementing this function.

CAUTION: Not following the documented guidelines could result in data loss.

CAUTION: To reduce the risk of data loss it is recommended that some level of fault tolerance be utilized in your RAID configuration. Refer to your Smart Array Controller user guide for information on fault tolerance options.

IMPORTANT: You must use Compaq Insight Manager and a Compaq Smart Array Controller to manage the drive array on your server if you wish to implement predictive failure alert.

Predictive Failure Replacement Guidelines

To minimize server downtime and data loss, use these guidelines when Compaq Insight Manager implements a predictive failure alert. The alert indicates that a drive is degraded and should be replaced.

- Ensure that all physical drives in the affected array are present and have the online LEDs illuminated before removing the degraded hot-plug drive. If any online LEDs are flashing (indicating a rebuild) or are not illuminated, the degraded drive must not be removed.

  For instructions on hot-plugging your hard drive, see the “Moving Drives” and “Replacing a Failed Drive and Using Spares” sections in Chapter 6, “Advanced Administrative Procedures.”

- Check for cabling configurations that are not supported. Signal integrity errors may be injected into the SCSI bus when an active drive is hot-plugged.

- Make sure fault tolerance is not currently being used to recover from errors to other drives in the array, such as media errors or signal integrity errors. Loss of fault tolerance following a drive replacement can result in problems.

CAUTION: In extreme cases, when the number of errors is greater than the firmware error recovery is able to sustain, hot-plugging an online drive may cause some unrecoverable errors to be reported to the operating system or may cause a complete failure of the array. Refer to your operating system documentation for more information on implications, as well as possible recovery options.

IMPORTANT: Before replacing a degraded hard drive, use Compaq Insight Manager to examine the error counters recorded for each physical drive in the array to verify that such errors are not presently occurring. Refer to the Compaq Insight Manager documentation on the Compaq Management CD.

SCSI Device Problems

If the SCSI device is not being recognized, make sure that it is configured correctly. Refer to the documentation provided with the SCSI device.

Hot-Plug Hard Drives

Make sure that the hot-plug hard drives are correctly and sequentially installed, starting with bay 0. It is not necessary to set the SCSI ID of a hot-plug hard drive. The backplane board automatically sets the ID when the drive is installed.

TaskSmart N2400 Server Troubleshooting

Table C-2
TaskSmart N2400 Server Troubleshooting

Problem	Recommended Action
The TaskSmart N2400 appliance does not power down.	Press and hold the power button for four seconds, and then release. This procedure invokes the hardware override for the power button.
The TaskSmart N2400 appliance is not working.	Most problems are caused by invalid IP address configurations. Three addresses are critical: a numeric IP address with a subnet mask, a valid gateway address on the same subnet as the IP address, and a valid DNS server IP address.
The TaskSmart N2400 appliance cannot be pinged from a client.	■ Verify that you are using the correct IP address and subnet mask for your network. ■ Make sure that all network cables are connected to the proper ports. ■ Check that all network connectors show a “link” connection.

Software and Firmware Diagnostic Tools

This section describes software and firmware diagnostic tools available for all Compaq server products. The topics covered in this section include:

- Default Configuration
- Running Compaq Utilities
- Diagnostics Software
- Array Diagnostic Utility
- Integrated Management Log
- Rapid Error Recovery
- Automatic Server Recovery-2
- ROMPaq Error Recovery Options
- ROMPaq Disaster Recovery

Default Configuration

The TaskSmart N2400 appliance ships with a default system configuration that defines operating system, storage, networking, and management settings. Unlike other Compaq server products, SmartStart is not used to set up and configure the TaskSmart N-Series appliance. The proper method for initializing and configuring the TaskSmart N2400 appliance is with a configuration data diskette produced by the TaskSmart Configuration Utility CD. The process for this method is described on the quick initialization and quick reference poster provided with the product.

If the server is mistakenly booted without using the configuration data diskette, the automatic system initialization process, called mini-setup, proceeds using built-in defaults for the hostname and other settings. After the Windows-based operating system boots, the initialization process detects that no configuration data diskette is present and presents the administrator with the following choices:

- **Verify—**allows the administrator to find or create the diskette and insert it, and then proceed with the remaining initialization items.
- **Ignore—**forces the initialization process to continue using defaults for any items that are not defined on the configuration diskette, or if there is no diskette.
- **Reset—**resets the appliance to its initial factory state, and the server powers down gracefully. The next time the server is powered up, the automatic mini-setup preparation process is initiated, allowing the administrator a second chance at creating and inserting a configuration diskette.

Additional server configuration methods include:

- System partition utilities, accessible by pressing the **F10** key during the boot sequence.
- Remote Insight Board configuration utilities, accessible by pressing the **F8** key when prompted during the boot sequence.

The TaskSmart N2400 appliance can be returned to factory default configuration at any time by utilizing the QuickRestore CD. OS Restore erases the current configuration of the appliance, reloading the operating system and all system software, including SWVR, ACU, and SFU. The Full Restore option erases the data drives as well, restoring their configuration to a factory-standard layout in terms of RAID arrays, pools, and virtual disks. QuickRestore can be data destructive. Read the QuickRestore guide carefully, and choose the appropriate options on the QuickRestore interface.

Inspect Utility

The Inspect Utility provides configuration information such as the contents of the operating system startup files, the current memory configuration, the ROM version, and Integrated Management Log (IML) information. The Inspect Utility operates with MS-DOS emulation mode of OS/2.

- Running the Inspect Utility

1. Power down the server, and then power it back up. Press the **F10** key when the cursor is displayed in the upper right corner of the screen.
2. At the main menu, select **Diagnostics and Utilities.**
3. Press **Enter.**
4. Select **Inspect Computer,** and then press **Enter.**

   NOTE: If Diagnostics is not installed on the hard drive, System Configuration prompts you to insert the Diagnostics diskette into drive A.

5. Follow the instructions displayed on the screen.

- Printing the Inspect listing

Select **Print** on the Inspect screen to print a copy of the Inspect listing. Keep a copy of the listing with each server for later reference.

Running Compaq Utilities

The Compaq SmartStart and Support Software CD contains the SmartStart program and many of the Compaq utilities needed to maintain the system, including:

- System Configuration Utility (SCU)
- Array Configuration Utility (ACU)
- Array Diagnostic Utility (ADU)
- Upgrade System Partition
- ROMPaq Firmware Upgrade Utilities
- Compaq Diagnostics

There are three ways to access Compaq utilities:

- From the Compaq System Partition
- From diskette
- From the Compaq SmartStart and Support Software CD

Running the Utilities on the Compaq System Partition

The Compaq utilities are automatically available on the Compaq system partition.

To run the utilities on the Compaq system partition, start the system, and then press the **F10** key when you see:

```
Press F10 for Compaq system partition utilities.
```

Then select the desired utility from the menu:

- The System Configuration Utility is available under the System Configuration menu.
- Compaq Diagnostics (Test and Inspect) are available under the Diagnostics and Utilities menu.
- The ROMPaq Firmware Upgrade Utility is available under the Diagnostics and Utilities menu.

Running the Utilities from Diskette

- Run the utilities from their individual diskettes. If you have a utility diskette newer than the version on the SmartStart and Support Software CD, use that diskette.
- Create a diskette version of the utility from the SmartStart and Support Software CD.

To create diskette versions of the utilities from the CD:

1. Start the Compaq SmartStart and Support Software CD.
2. From the Compaq System Utilities screen, select **Create Support Software Disks,** and then **Next.**
3. Select the diskette that you would like to create from the list, and then follow the instructions on the screen.

Running the Utilities from the Compaq SmartStart and Support Software CD

IMPORTANT: SmartStart is not used to configure the server. The server is preconfigured. Use the QuickRestore CD for server configuration.

To run these utilities directly from the Compaq SmartStart and Support Software CD:

1. Start the Compaq SmartStart and Support Software CD.
2. From the Compaq System Utilities screen, select the utility that you want to run, and then select **Next.**

Diagnostics Software

Test Error Codes tables include all test error codes generated by Compaq products. Each code has a corresponding description and recommended action or actions. Each system generates only those codes that apply to its configuration and options.

When you select Diagnostics and Utilities from the System Configuration Utility main menu, the utility prompts you to test, inspect, upgrade, and diagnose the server.

Diagnostics and Utilities are located on the Compaq system partition on the hard drive and must be accessed when a system configuration error is detected during the Power-On Self-Test (POST). Compaq Diagnostics software is also available on the Compaq SmartStart and Support Software CD. You can create a diagnostics diskette from the SmartStart and Support Software CD and run Diagnostics from diskette. See the procedure in the “Running Compaq Utilities” section earlier in this appendix.

> **NOTE:** The Enable Drive A: Boot feature must be set before diagnostics can be accessed from a diskette.

The following options are available from the Diagnostics and Utilities menu:

- Test Computer
- Inspect Computer
- Upgrade Firmware
- Remote Utilities

Diagnostic error codes are generated when the Diagnostics software recognizes a problem. These error codes help to identify possible defective subassemblies.

Steps for Diagnostics

In Table C-3, the “Recommended Action” column lists the steps necessary to correct a problem. After completing the steps listed in the table, run the Diagnostics Utility to verify that the error condition has been corrected. If the error code is redisplayed:

1. Perform the next step listed in the table.
2. Run the Diagnostics program again.
3. Follow this procedure until the Diagnostics program no longer detects an error condition.

Table C-3
Primary Processor Test Error Codes

Error Code	Description	Recommended Action
101-*XX*	CPU test failed.	1. Replace the processor and retest. 2. Replace the system board and retest.
103-*XX*	DMA page registers test failed.	Replace the system board and retest.
104-*XX*	Interrupt controller master test failed.	
105-*XX*	Port 61 error occurred.	
106-*XX*	Keyboard controller self-test failed.	
107-*XX*	CMOS RAM test failed.	1. Replace the battery/clock module and retest. 2. Replace the system board and retest.
108-*XX*	CMOS interrupt test failed.	
109-*XX*	CMOS clock load data test failed.	
110-*XX*	Programmable timer load data test failed.	Replace the system board and retest.
111-*XX*	Refresh detect test failed.	
112-*XX*	Speed test slow mode out of range.	
113-*XX*	Protected mode test failed.	
114-*XX*	Speaker test failed.	1. Verify the speaker connection and retest. 2. Replace the speaker and retest. 3. Replace the system board and retest.
116-*XX*	Cache test failed.	Replace the processor and retest.

continued

Table C-3
Primary Processor Test Error Codes *continued*

Error Code	Description	Recommended Action
122-*XX*	Multiprocessor dispatch test failed.	1. Check the system configuration and retest. 2. Replace the processor and retest. 3. Replace the system board and retest.
123-*XX*	Interprocessor communication test failed.	
199-*XX*	Installed devices test failed.	1. Check the system configuration and retest. 2. Verify cable connections and retest. 3. Check switch or jumper settings, or both, and retest. 4. Run the BIOS Setup Utility and retest. 5. Replace the processor and retest. 6. Replace the system board and retest.

Array Diagnostic Utility

Array Diagnostic Utility (ADU) is a Windows-based software tool designed to run on all Compaq servers that support Compaq Array Controllers and are running SmartStart 4.10 or later. The two main functions of ADU are to collect all possible information about array controllers in the system and to generate a list of detected problems. The error messages and codes listed include all codes generated by Compaq products. The system generates only codes applicable to the configuration and options in the server.

ADU works by issuing multiple commands to the array controllers to determine if a problem exists. This data can then be saved to a file. In severe situations, this file can be sent to Compaq for analysis. In most cases, ADU provides enough information to initiate problem resolution immediately.

NOTE: ADU does not write to the drives, destroy data, or change or remove configuration information.

Starting ADU

CAUTION: Do not cycle the power during this process. ADU must perform low-level operations that, if interrupted, could cause the controller to revert to a previous level of firmware if the firmware was soft-upgraded.

1. Insert the Compaq SmartStart and Support Software CD into the CD-ROM drive.
2. Restart the system from the SmartStart CD.
3. Select **ADU** from the System Utilities menu.

A Please Wait panel is displayed, indicating that ADU is identifying the system parameters. ADU gathers information from all of the array controllers in the system. The time that it takes to gather this information depends on the size of the system. When the information-gathering process is complete, the main screen or a panel indicating any problems detected is displayed.

To generate an ADU report, select **File,** and then **Save Data** from the Command menu.

Integrated Management Log

The Integrated Management Log (IML) records system events and stores them in an easily viewable form. Each event is marked with a timestamp with one-minute granularity.

Events listed in the IML are categorized as one of four event severity levels:

- **Status—**indicates that the message is informational only.
- **Repaired—**indicates that corrective action has been taken.
- **Caution—**indicates a nonfatal error condition.
- **Critical—**indicates a component failure.

The IML requires operating system-dependent drivers from Compaq. Refer to the Compaq Support Software CD for instructions on installing the appropriate drivers.

Viewing the Log

You can view an event in the IML in several ways:

- From within Compaq Insight Manager
- From within the Compaq Survey Utility
- From within the IML Management Utility

Compaq Insight Manager

Compaq Insight Manager is a comprehensive management tool used to monitor and control the operation of Compaq servers and clients. Compaq Insight Manager consists of two components: a Windows-based console application, and server- or client-based management data collection agents. Starting with Compaq Insight Manager 4.0, the agents for Windows NT and NetWare are also Web-enhanced; that is, these agents enable Web browser access and monitoring of management information.

The management agents monitor over 1,000 management parameters. Key subsystems are instrumented to make health, configuration, and performance data available to agent software. Agents act upon data by initiating information, such as statistics on network interface or storage subsystem performance.

Viewing the Event List

1. From Compaq Insight Manager, select the appropriate server, and then select **View Device Data**. The selected server is displayed, with buttons around the perimeter.
2. Select **Recovery,** and then **Integrated Management Log.**
3. If a failed component has been replaced, select the event from the list. Then select **Mark Repaired.**

NOTE: You can view the event list only from the Recovery/Integrated Management Log screen as described in the previous steps.

Printing the Event List

1. From the Compaq Insight Manager screen, select the appropriate server.
2. Select **Configuration,** then **Recovery,** and then **Print.**

Compaq Survey Utility

The Compaq Survey Utility is a serviceability tool. It delivers online-configuration capture and comparison to maximize server availability. It is delivered on the Compaq Management CD in the SmartStart package, or is available on the Compaq website. Refer to the Compaq Management CD for information on installing and running the Compaq Survey Utility.

After running the Compaq Survey Utility, view the IML by loading the output of the utility (typically called *SURVEY.TXT*) into a text viewer such as Microsoft Notepad. The event list follows the system slot information. After opening the text file, print it using the print feature of the viewer.

Compaq IML Management Utility

The Compaq IML Management Utility is a DOS-based tool that gives you the offline ability to review, mark corrected, and print events from the IML. It is located on the Compaq SmartStart and Support Software CD. Refer to the SmartStart Installation for Servers poster, which ships with the server, for information on how to install and use the IML Management Utility.

Event List

In the Event List the affected components and the associated error messages are displayed. Though the same basic information is displayed, the format of the list may differ, depending on how you view it: on the IML, from within Compaq Insight Manager, or from within the Compaq Survey Utility. An example of the format of an event displayed on the IML is as follows:

```
**001 of 010**
---caution---
03/19/1997
12:54 PM
FAN Failure
Main System
Location:
System Board
Fan ID: 03
**END OF EVENT**
```

Rapid Error Recovery

Compaq servers provide rapid recovery services for diagnosing and recovering from errors. These tools are available for local and remote diagnosis and recovery.

Rapid recovery means fast identification and resolution of complex faults. The Rapid Recovery Engine and Compaq Management Agents for Servers notify the system administrator when a failure occurs, ensuring that the server experiences minimal downtime. You enable these features through the System Configuration Utility. These integrated server management features are:

- Automatic Server Recovery-2 (ASR-2)
- Integrated Management Logs (IMLs)
- Storage Fault Recovery Tracking
- Storage Automatic Reconstruction (requires the Integrated Smart Array Controller)
- Network Interface Fault Recovery Tracking
- Memory Fault Recovery Tracking

Automatic Server Recovery-2

Automatic Server Recovery-2 (ASR-2) lets the server restart automatically from the operating system or the Compaq Utilities. To use this feature, you must use the System Configuration Utility to install Compaq Utilities in the Compaq system partition.

You can enable the ASR-2 feature to restart a server after a critical hardware or software error occurs. If a critical error occurs, the server records the error information in the IML, restarts the system, and pages you. Using the Compaq System Configuration Utility, configure the system for automatic recovery or for attended local or remote access to diagnostic and configuration tools.

You can also configure ASR-2 to page an administrator when the system restarts. ASR-2 depends on the application and driver that routinely notify the ASR-2 hardware of proper system operations. If the time between ASR-2 notifications exceeds the specified period, ASR-2 determines that a fault has occurred and initiates the recovery process.

To configure ASR-2:

1. Run the System Configuration Utility.
2. Select **Configure Computer.**
3. Select **View and Edit Details.**
4. Set the software error recovery status to **Enabled.**
5. Set the software error recovery timeout.

The available recovery features are:

- **Software Error Recovery—**can be set to automatically restart the server after a software-induced server failure.
- **Environmental Recovery—**can be set to allow the server to restart when temperature, fan, or AC power conditions return to normal.

Unattended Recovery

For unattended recovery, ASR-2 performs the following actions:

- Logs the error information to the IML
- Resets the server
- Pages you (if a modem is present and you selected Paging)
- Tries to restart the operating system

Often the server successfully restarts, making unattended recovery the ideal choice for remote locations where trained service personnel are not immediately available.

If ASR-2 cannot restart the server within 10 attempts, ASR-2 places a critical error message in the IML, starts the server into Compaq Utilities, and enables remote access (if you configured remote access).

To use this level of ASR-2, you must configure ASR-2 to load the operating system after restart.

Attended Recovery

For attended recovery, ASR-2 performs the following actions:

- Logs the error information to the IML
- Resets the server
- Pages you (if a modem is present and you selected Paging)
- Starts Compaq Utilities from the hard drive
- Enables remote access

During system configuration, these utilities are placed on the system utilities partition of the hard drive.

If you have configured for dial-in access and have a modem with an auto-answer feature installed, you can dial in and remotely diagnose or reconfigure the server.

If you have configured the Compaq Utilities for network access, you can access the utilities over the network. You can use Compaq Insight Manager for dial-in or network access.

Hardware Requirements

You can also run Compaq Utilities remotely over an IPX or IP network using the Network feature:

- To use Compaq Utilities on an IPX network, you must have Compaq Insight Manager 2.0 or later, or an NVT (Novell Virtual Terminal) Terminal Emulator with VT100 or ANSI terminal capabilities.
- To use Compaq Utilities on an IP network, you must have Compaq Insight Manager 2.10 or later, or a Telnet Terminal Emulator with VT100 or ANSI capabilities.

If you are notified that ASR-2 restarted the server and you have restarted to Compaq Utilities, use the Inspect Utility or Compaq Insight Manager to view the critical error. Run Diagnostics to diagnose and resolve the problem.

You can configure ASR-2 to restart the server into Compaq Utilities to diagnose the critical error or to start the operating system to return the server to operational status as rapidly as possible.

When you enable ASR-2 to start the operating system, the server tries to start from the primary partition. In this mode, ASR-2 can page you if a critical error occurs, but you cannot access Compaq Utilities.

When you enable ASR-2 to start Compaq Utilities, the server restarts after a critical error and loads Compaq Utilities from the Compaq system partition on the hard drive.

ASR-2 Integrated Management Log Messages

The IML records memory errors, as well as catastrophic hardware and software errors that cause the system to fail. This information helps you to quickly identify and correct the problem, thus minimizing downtime.

You can view the IML through Compaq Insight Manager. The Diagnostics Utility either resolves the error or suggests corrective action in systems that do not support event logs.

The IML identifies and records all the following errors as defined in Table C-4.

Table C-4
ASR-2 Features

Features	Definition
Software error recovery	If enabled, ASR-2 is activated if the OS stops responding.
Software error recovery timeout	Determines how long the server waits to enable ASR-2 after an OS lockup.
Standby recovery server option	If enabled, ASR-2 activation initiates a switch to a standby recovery server.
Standby recovery server port	Port used to communicate with the recovery server.
Standby recovery timeout	Determines how long the server waits to initiate switch after ASR-2 activation.
Software error recovery start option	Allows the server to restart either into the OS or into Compaq Utilities.
Thermal shutdown	If enabled, shuts down the server if a critical thermal error occurs.
UPS shutdown	If enabled, allows the server to perform a shutdown if a UPS is activated.
UPS shutdown threshold	Determines how long the server waits to shut down after the UPS is activated. If desired, this number should provide enough time for an administrator to perform any necessary operations or to gracefully shut down the server.

Compaq Integrated Remote Console

The standard Compaq Integrated Remote Console performs a wide range of configuration activities. Console features are as follows:

- Is accessible using ANSI terminal
- Operates independently of the operating system
- Provides for remote server restart
- Provides access to system configuration
- Uses out-of-band communication with dedicated management modem installed in the server

Compaq Health Driver

The Compaq Health Driver continually resets the ASR-2 timer according to the frequency that you specified in the System Configuration Utility (for example, 10 minutes). If the ASR-2 timer counts down to zero before being reset due to an operating system fatal error or a server lock-up, ASR-2 restarts the server into either Compaq Utilities or the operating system (as indicated by the System Configuration parameters). The default value is 10 minutes. The allowable settings are 5, 10, 20, and 30 minutes.

For remote and offsite (unattended) servers, setting the software error recovery timeout for 5 minutes reduces server downtime and allows the server to quickly recover. For local (attended) servers located onsite, you can set the software error recovery timeout for 20 or 30 minutes, giving you time to arrive at the server if you wish to manually diagnose the problem.

The Compaq Health Driver is independent of the ASR-2 timer. You must load it and enable the ASR-2 timer. Then the driver detects and logs information in the IML regarding numerous hardware and software errors. However, you cannot enable the ASR-2 timer without first loading the Health Driver.

Before ASR-2 restarts the server, ASR-2 records any information available about the condition of the operating system in the IML. This information can be used to diagnose an operating system nonresponse or server lock-up while still allowing the server to be restarted.

The following ASR-2 flowchart shows you the sequence of events after a hardware or software error occurs.

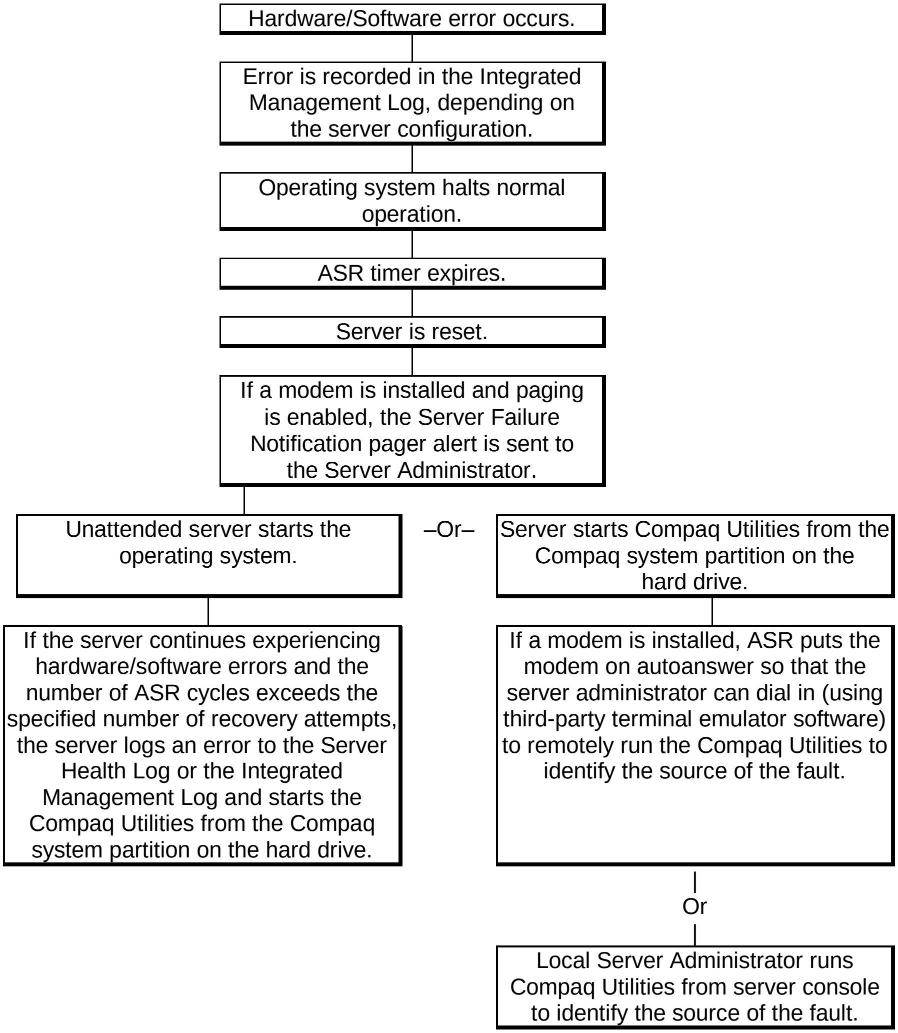

Hardware/Software error occurs.
Error is recorded in the Integrated Management Log, depending on the server configuration.
Operating system halts normal operation.
ASR timer expires.
Server is reset.
If a modem is installed and paging is enabled, the Server Failure Notification pager alert is sent to the Server Administrator.
Unattended server starts the operating system.
–Or–
Server starts Compaq Utilities from the Compaq system partition on the hard drive.
If the server continues experiencing hardware/software errors and the number of ASR cycles exceeds the specified number of recovery attempts, the server logs an error to the Server Health Log or the Integrated Management Log and starts the Compaq Utilities from the Compaq system partition on the hard drive.
If a modem is installed, ASR puts the modem on autoanswer so that the server administrator can dial in (using third-party terminal emulator software) to remotely run the Compaq Utilities to identify the source of the fault.
Or
Local Server Administrator runs Compaq Utilities from server console to identify the source of the fault.

Figure C-1. ASR-2 flowchart

Starting into Compaq Utilities

When you enable ASR-2 to start into Compaq Utilities and a critical error occurs, the operating system-specific Health Driver logs the error information in the IML and the ASR-2 feature restarts the server. When the system reinitializes, the system pages the designated administrator (if enabled), and starts Compaq Utilities from the hard drive.

If Dial-In status is enabled, the modem is placed in autoanswer mode. If you enable Dial-Out status, you are automatically enabled for Dial-In.

If Network Status is enabled, the appropriate network support software is loaded, depending on the network protocol, IP or IPX. The Network Status allows remote access through the network.

IMPORTANT: Compaq Utilities are loaded from a specially created Compaq system partition on the hard drive. This partition was configured during server configuration.

You can access the server and view the IMLs remotely by modem, in-band over the network, or directly from the server. For modem access, you must have either Compaq Insight Manager 2.0 or above or have a VT100 or ANSI terminal type device. You can use a standard CRT with VT100 or ANSI emulation capability, or you can use a PC with a VT100 or ANSI terminal emulation package. The communication parameters must be set for 8 data bits, no parity, and 1 stop bit.

You can also enable ASR-2 to allow network access using the Network Status feature in the System Configuration Utility. You must have either Compaq Insight Manager 2.0 or greater or an NVT emulator on an IPX network to use this feature. You must also have Version 2.24 or later of the System Configuration Utility. For IP access, you must have Compaq Insight Manager 2.10 or later, or a Telnet Terminal emulator to use this feature. You also must have Version 2.24 or later of the System Configuration Utility.

If you configure the server to start into Compaq Utilities, the server prepares for remote communications. You can remotely run Diagnostics software, the Inspect Utility, or the System Configuration Utility using a workstation running terminal emulation software, such as Compaq Insight Manager or PC Anywhere.

Starting into the Operating System

When you enable ASR-2 to restart into the operating system and a critical error occurs, ASR-2 logs the error in the IML and restarts the server. The system ROM pages the designated administrator, and then executes the normal restart process.

IMPORTANT: When you enable ASR-2 to restart into the operating system, Modem Dial-In Status, Network Status, and Modem Dial-Out Status are automatically disabled. In this mode, ASR-2 can page you if a critical error occurs, but you cannot access the server, and the server cannot dial out to a remote workstation.

If the ASR-2 feature cannot restart the server within 10 attempts, ASR-2 logs a critical error in the IML and restarts the server into the Compaq Utilities, and then puts the modem into auto-answer mode.

ROMPaq Error Recovery Options

The process of upgrading the system ROM is referred to as flashing the ROM. Flashing consists of using software to replace the current ROM image with a new one through ROMPaq.

Should an error such as a power failure occur during this process, the flash operation is not completed, causing the ROM image in the server to be corrupted. Compaq provides two options for ROMPaq recovery, depending on the server and circumstances involved.

ROMPaq Disaster Recovery

The following option must be utilized by any server that does not have a valid ROM image.

1. Build a fresh ROMPaq diskette, using the latest version for the server involved.

   NOTE: If the ROM is corrupted by a ROMPaq interruption, the initial ROMPaq attempt may have affected the contents of the original diskette.

2. Power down the server.
3. Set configuration switches 1, 4, 5, and 6 on the system maintenance switch block to On to enable disaster mode.
4. Insert the ROMPaq diskette. Although you utilize a normal ROMPaq diskette, this situation does not allow you to save the old image.

5. Power down the server. The keyboard, mouse, and monitor are all inactive.
6. The server emits two long beeps to indicate that you are in Disaster Recovery mode and that you should insert the ROMPaq diskette.
7. The server reads the diskette for the latest ROM image. If the diskette is not in place, the system continues to beep until a valid ROMPaq diskette is inserted.
8. After successful completion of this process:
    a. Power down the server.
    b. Remove the diskette.
    c. Reset configuration switches 1, 4, 5, and 6 (see Table C-5).
    d. Power up the server as usual.
    e. After a failed ROMPaq, power down the server, and then repeat the above process.

Table C-5
Configuration Switches

Switch	Function
1	Disable on-board graphics
4	Disable diskette drive
5	Disable password
6	Clear NVRAM

SFU Troubleshooting

A user cannot access an export.

Is the folder exported? Execute "showmount –e servername" to see if the export name is listed. If not, the directory is not being exported out. Export out the directory using NFS. .

Does the client have permission to access the share? Check permissions listed on the share from the showmount –e command (above). If the client (by name, IP address, or "Everyone") does not have access to the share, edit the permissions on the share to allow the client access

Does the user have permission to the directory or file that they are trying to access? Check the ACL (or UNIX permissions listing) on the directory or file. If the mapped user does not have access to the file and should have access, change the permissions to allow the mapped user access.

Users are displayed as "nobody," "nogroup," or both.

Are the user and group correctly mapped? Check the ACL and the user mappings under the SFU MMC module. Verify that the UNIX user and group are mapped to the correct NT user and group. If not, adjust the mappings accordingly.

Is the user mapping service running? Check the service in the SFU MMC, the services MMC, or both. If the service is not running, start it in the SFU MMC. Check the event log for error messages, to see why the user mapping service is not running.

Users are displayed as incorrect users, or have access to files they should not, or both.

Is the user correctly mapped? Go into the SFU MMC, User Name Mapping section, and check the advanced maps. If the user is mapped to an incorrect entry, change the name to the correct entry.

Is simple mapping on? Check in the SFU MMC, User Name Mapping section, and see if “simple mapping” is checked. If so, enable the “display simple maps” check box, and look in the user mappings control list. See if the user is mapping to an incorrect entry. If so, implicit mapping is the problem, because the username matches spelling to an incorrect user. Change the name on the UNIX side, or turn off simple mappings, which requires all users to be explicitly mapped.

“RPC: procedure call failed” error occurs when a “showmount” or other command is executed.

Is the NFS service running? Check the event log for the message stating that the NFS service has started. If not, this is the cause of the problem. Wait for the machine to finish powering up. If the event log entry is present, check the service display in the MMC. If the service is not running, this is the cause of the problem.

When mounting a share on a client machine as root, permission denied errors are displayed, or new files are listed as “nobody.”

Does the share have “root” permissions enabled for that client? Check the share permissions. An entry for “root” permissions has to exist for that specific client listed in the permissions. If not, the “root” user is always squashed to “nobody,” although the group may still map to “root.” This omission affects a user’s permissions and access.

When mounting a share on a client machine as root, and “ls –al” denotes the mount point directory, a total of 0 files is reported and the “.” and “..” directories cannot be seen. When I attempt to create a file, I get a “permission denied” error message.

FAT32 filesystems are currently not supported for SFU NFS sharing. Only NTFS filesystems are supported as NFS shares. The only solution is to disable the NFS share, convert the filesystem to NTFS, and then re-enable the share.

The share was created **not** to allow anonymous share access. Anonymous access is given by default when the user interface is used. Anonymous share access can also be created by using the command line by typing:

```
nfsshare sharename=drive letter:\path –o anon
```

I created a shared folder, and then renamed or deleted it. Now it seems to no longer be NFS shared, yet the old share name is still showing on the server.

You need to always stop NFS sharing before renaming or deleting folders that are NFS shared. To clean out the old share, you need to go to a command prompt and run:

```
“nfsshare /d <alias name>”
```

This step deletes the old alias.

I created a folder with spaces in its name, and shared it out successfully with CIFS. But when I shared it out using NFS, the alias name contains underscores instead of spaces.

This behavior is expected for SFU NFS. Because not all UNIX clients can handle spaces in the alias names, SFU automatically translates spaces into underscores. SFU does not allow spaces in an alias name, and gives an error message when you attempt to re-enter the spaces.

When I attempt to share out a directory, an error message is displayed saying that a parent or child directory is already shared out, and it will not let me share this directory.

This behavior is expected for SFU NFS.

If a higher-level (parent) directory is already shared out, you cannot share out a subdirectory, because direct mounting of subdirectories is already supported. The correct usage is to mount the full path from the parent share. For example, if directory “/Data” is already shared out, you cannot share out “/Data/Accounting/Fred.” You can already directly mount “/Data/Accounting/Fred” just by sharing out “/Data.” .

If a lower-level (child) directory is already shared out, you cannot share out the parent (higher-level) directory. See the previous discussion about parent directories. SFU NFS already supports sharing out child directories from a parent. To share out this higher-level directory, you need to disable all lower directory shares, and then enable this directory for NFS sharing

I can map multiple Windows users to a single UNIX user. However, when I try to map several UNIX users to a single Windows users I get an error.

This behavior is expected. Services for UNIX does not support mapping multiple UNIX users to a single Windows user.

The server shows a mount for a client that is logged out.

Did the client unmount before logging out? The client must log on again, unmount the share, and then log off. The client can also restart the machine to break the mount.

> **NOTE:** Only the root on a UNIX system can unmount NFS shares unless the UNIX system administrator has built a script or other tool to allow other users to unmount NFS shares in root user context.

When I try to mount from a UNIX client, I get one of the following errors:

- Mount failed:permission denied

  Did you type the NFS export name correctly? The NFS export name is case sensitive.

  Does the client have permission to access the export? If the client does not have permission to access the export, or if the client does not have permission to access the TaskSmart N2400 appliance, the client cannot mount the NFS export.

- The client machine ceases operation on the command cursor.

  Did you type the correct IP address for the NFS server? If you are not using the UNIX hosts file for naming resolution, be sure that you typed in the correct NFS server IP address.

  Is the NFS server online? Make sure that the server is online before a mount is processed. This whether the server is online by issuing a ping or showmount command from the client to the server.

  Mount: can’t get an address for *incorrect servername*

  Did you type the correct NFS servername? The name must be typed exactly as it is listed in the UNIX hosts file or the Domain Name Server.

  Mount: RPC:Program not registered

  Is Server for NFS started? Start the service, right-click **Server for NFS** in the MMC, and then select **Start** or type at the command prompt:

  ```
  net start “Server for NFS”
  ```

Mappings do not reflect changes made to advanced user and group mapping.

The User Mapping Server has not refreshed the new mappings. The cache refresh rate by default is set to update every 30 (1,800 decimal) minutes. This rate can be changed with a registry edit. The location is:

HKEY_LOCAL_MACHINE\Software\Microsoft\Server for NFS\CurrentVersion\Mapping
“CacheRefresh.”

The possible refresh rates range from a minimum of 15 minutes to a maximum of 24 hours.

NOTE: Setting the refresh rate too low can affect performance due to the frequency of the updates.

The NFS Server can be refreshed immediately by running the Refresh NFS Server Setting script in the SFU section of the MMC or by stopping the NFS service and the User Mapping service. Restart the user Mapping service, and then restart the NFS Service. Restarting the TaskSmart N2400 appliance also accomplishes the same thing.

NOTE: Notify all users that are connected before stopping any services.

Stopping and Starting NFS File Service

There are two ways to start or stop NFS service on the TaskSmart N2400 appliance:

- From the Microsoft Management Console (MMC)
- From the command line

IMPORTANT: Before stopping the service, be sure to provide advance warning to users so that they may save their work.

Use the following procedures to stop and restart the NFS file server.

Stopping and Starting NFS from the MMC

1. Log on to the TaskSmart server as Administrator.
2. Click **Microsoft Management Console.**
3. Click **Services for UNIX.**
4. Right-click **Server for NFS.**
5. *To STOP*: Highlight and click **Stop.** If Stop is not available, the service is not currently running.
6. *To START*: Highlight and click **Start.** If Start is not available, it means that the service is already running.

Stopping and Starting NFS from the Command Line

1. Log in to the TaskSmart server as Administrator.
2. Click **Manage with Command Line.**
3. *To STOP*: From the command prompt, enter the following:

   ```
   net stop “Server for NFS”
   ```

4. *To START*: From the command prompt, enter the following:

   ```
   net start “Server for NFS”
   ```

Network Interface Controller Troubleshooting

This sections lists problems and outlines steps to take for resolving problems with either the standard NC3132 and NC3134 network interface controllers (NICs) or the optional NC6132 Gigabit Fibre NIC. Because of the graphics needed for this troubleshooting section, an overall table format is not used to list the information.

The NIC Cannot Connect to the Network

1. **Make sure that the cable is properly installed.**

   The network cable must be securely connected at both the NIC and the switch. This requirement applies to the NC6132, NC3132 and NC3134. If the cable is attached and the distance is within acceptable limits (100 meters for copper) but the problem persists, try a different cable. If you are directly connecting two computers (no hub or switch), use a crossover cable.

   For more information regarding the NC6132 about crossover cables and acceptable lengths for cables, refer to the *Readme* file on the *Software and Documentation* CD that comes in the NC6132 Gigabit NIC package

2. **Check the LEDs on the NIC using Table C-6 and Table C-7.**

Table C-6
NC3132 and NC3134 NIC LEDs

LED	Indication	Meaning
LNK	On	The NIC and hub are receiving power. The cable connection between the hub and NIC is good.
	Off	The NIC and hub are not receiving power, or the cable connections between the hub and NIC is faulty.
ACT	On or flashing	The NIC is sending or receiving network data. The frequency of the flashes varies with the amount of network traffic.
	Off	The NIC is not sending or receiving network data.
100	On	The NIC is operating at 100 megabits per second (Mbps).
	Off	The NIC is operating at 10 Mbps.

Table C-7
NC 6132 NIC LEDs

LED	Indication	Meaning
LNK	On	The NC6132 and hub are receiving power. The cable connection between the hub and Gigabit NIC is good.
	Off	The NC6132 and hub are not receiving power, the cable connection between the Gigabit NIC and hub is faulty, or there is a driver configuration problem.
ACT	On or flashing	The NC6132 is receiving direct packets or broadcast packets for this specific NIC. When sending packets, the ACT LED is also active due to network acknowledgements received.
	Off	The NC6132 is not receiving direct packets or broadcast packets.

3. **Make sure that the switch port and the NIC have the same speed and duplex settings.**

   If you configured the NIC for full duplex, make sure the switch port is also configured for full duplex. Setting the wrong duplex can degrade performance, cause data loss, or result in loss connections. Also, make sure that if you are running at 100 Mbps, that the switch supports this speed.

   NOTE: These settings do not apply for the Gigabit Fibre adapters.

4. **Reseat the NIC and upgrade module (daughter board).**

   Open up the unit and reseat both the NIC and the upgrade module making sure that they are making a good firm connection.

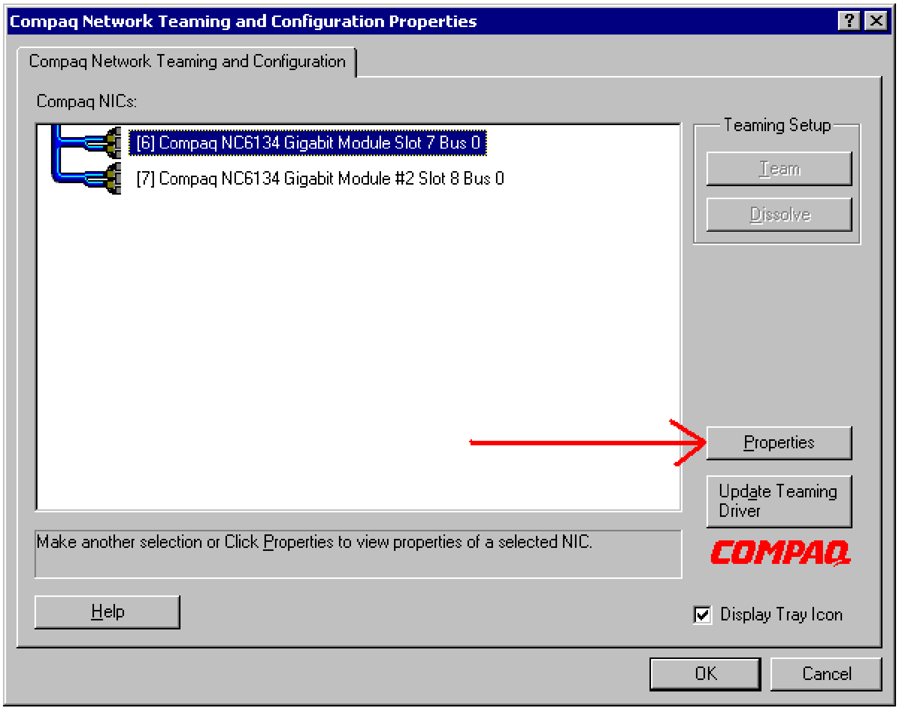
5. **Test the network interface controllers using Compaq Diagnostics.**

   To run the NIC diagnostics you must first install the Network Teaming utility. Double click the **CPQTEAM Setup** icon located on the desktop and follow the installation instructions.

   After the utility is installed, the **CPQTEAM** icon is displayed in the desktop tray. Double click this icon to run *CPQTEAM*.

Next, highlight the Network adapter that you are having problems with, and then click **Properties**.

> **NOTE:** The network adapters shown in the figure below may differ from the network adapters installed on your system.



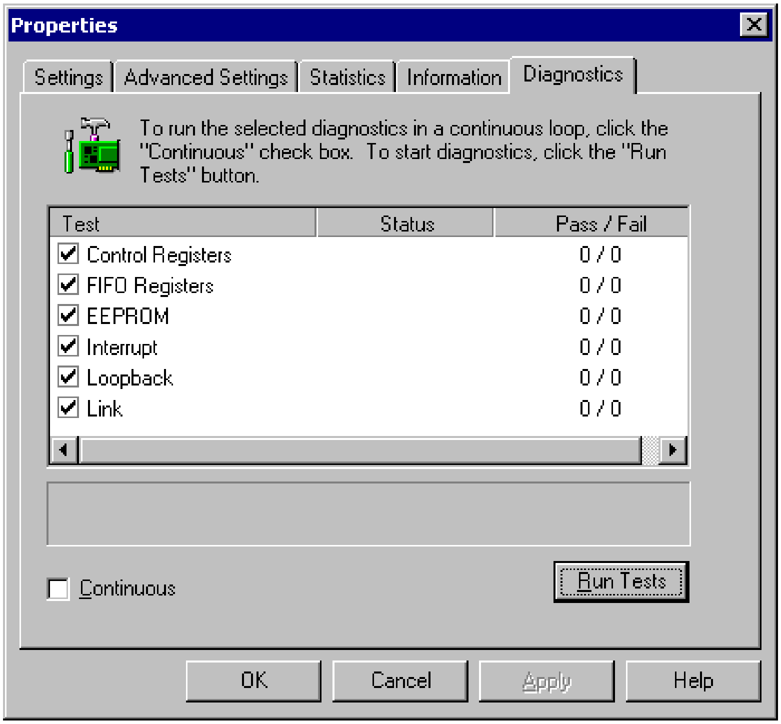
Compaq Network Teaming and Configuration Properties
Compaq Network Teaming and Configuration
Compaq NICs:
[6] Compaq NC6134 Gigabit Module Slot 7 Bus 0
[7] Compaq NC6134 Gigabit Module #2 Slot 8 Bus 0
Teaming Setup
Team
Dissolve
Properties
Update Teaming Driver
COMPAQ
Help
Display Tray Icon
OK
Cancel

Make another selection or Click Properties to view properties of a selected NIC.

☑ Display Tray Icon

Figure C-2. Compaq Network Teaming and Configuration Properties screen

Under **Properties**, select the **Diagnostics** tab, and then click on **run tests**. A warning appears telling you that running this application will disconnect you from the network; click **OK**.



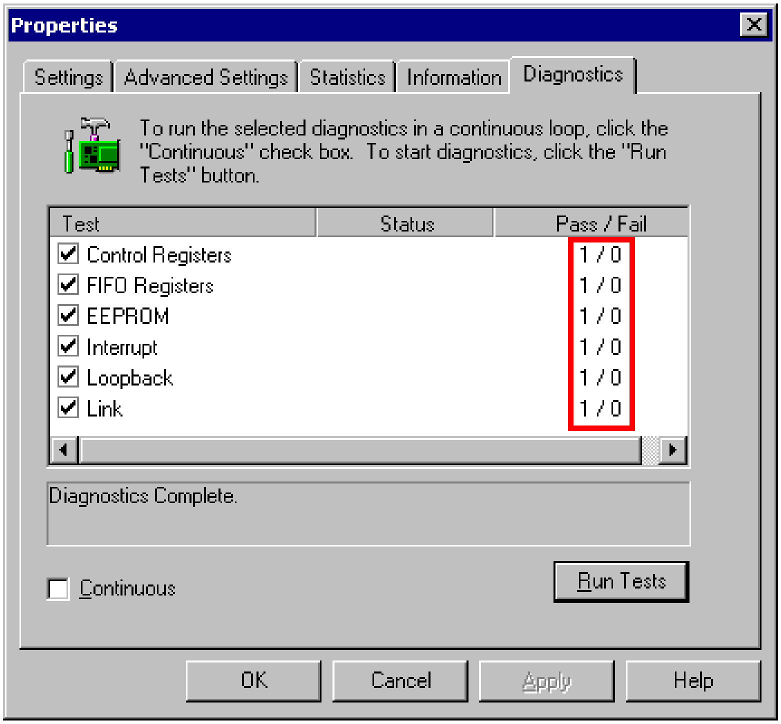
To run the selected diagnostics in a continuous loop, click the "Continuous" check box. To start diagnostics, click the "Run Tests" button.

Test	Status	Pass / Fail
☑ Control Registers		0 / 0
☑ FIFO Registers		0 / 0
☑ EEPROM		0 / 0
☑ Interrupt		0 / 0
☑ Loopback		0 / 0
☑ Link		0 / 0

☐ Continuous

Figure C-3. Compaq Network Teaming and Configuration Properties screen Diagnostic tab

After it completes testing, the results should look like the following. If not, there is a problem with either the settings or the Network Adapter itself.



To run the selected diagnostics in a continuous loop, click the "Continuous" check box. To start diagnostics, click the "Run Tests" button.

Test	Status	Pass / Fail
☑ Control Registers		1 / 0
☑ FIFO Registers		1 / 0
☑ EEPROM		1 / 0
☑ Interrupt		1 / 0
☑ Loopback		1 / 0
☑ Link		1 / 0

Diagnostics Complete.

☐ Continuous

Figure C-4. Compaq Network Teaming and Configuration Properties screen Diagnostic tab test results

Other Common Network Interface Controller Problems and Solutions

Diagnostics pass, but the connection fails or errors occur.

1. At 100Mbps, use Category 5 wiring and make sure the network cable is securely connected.
2. For NetWare clients, make sure that you specify the correct frame type in your *NET.CFG* file.
3. Make sure that the duplex mode setting on the NIC matches the setting on the hub.
4. At 100Mbps, connect to a 100BASE-TX hub only (not 100BASE-T4).
5. The NIC device driver may be faulty. Re-install the driver and check the connection.
6. The Unit IP address does not match the network subnet mask that it is connected to.
7. The NIC “software” MAC address already corresponds to an existing MAC address out on the network.
8. TCP/IP protocol is not installed to the network stack yet.
9. The NIC set up for DHCP cannot talk to the DHCP server. The user needs to use a static IP address.

The LNK LED does not light.

1. Check all connections at the NIC and the hub.
2. Try another port on the hub.
3. Make sure the duplex mode setting on the NIC matches the setting on the hub.
4. Make sure that you have the correct type of cable between the NIC and the hub. 100BASE-TX requires two pairs. Some hubs require a crossover cable, and others require a straight-through cable. Refer to the “Cabling Information” *Readme* file for more information on cabling.

The ACT LED does not light.

1. Make sure that you have loaded the correct network drivers.
2. The network may be idle. Try accessing a server.
3. The NIC is not transmitting or receiving data. Run diagnostics, and then try another NIC.
4. Make sure to use two-pair cable for TX wiring.

The NIC stopped working when another NIC was added to the computer.

1. Make sure the cable is connected to the NC3120 NIC.
2. Try reseating the newest NIC.

The NIC stopped working without apparent cause.

1. Run the diagnostics.
2. Try reseating the NIC first, and then try a different slot if necessary.
3. The network driver files may be corrupt or deleted. Delete and then reinstall the drivers.

Remote Insight Lights-Out Edition Board Troubleshooting

This section contains the following Remote Insight Lights-Out Edition board troubleshooting topics:

- Resetting the Remote Insight Lights-Out Edition Board
- Troubleshooting Logon Problems
- Troubleshooting Alert and Trap Problems
- Miscellaneous Remote Insight Lights-Out Edition Board Troubleshooting

Resetting the Remote Insight Lights-Out Edition Board

There are various times when you may need to reset the Remote Insight Lights-Out Edition board. .

To reset the Remote Insight Lights-Out Edition board, follow these steps:

1. Right-click the **My Computer** icon of your desktop, and then select **Manage.**
2. Expand the **Services and Applications** folder.
3. Select **Services**.
4. Stop the Compaq Server Agents service. This action stops the Compaq Remote Insight Board Configuration agent, the Compaq Web Agent, and the Compaq Foundation Agents.
5. In Control Panel, select the **Compaq Management Agents** applet.
6. Select the **Remote Insight** tab, and then click the **Reset Remote Insight Board** button.
7. Restart the Compaq Server Agents service

Troubleshooting Logon Problems

Logon name and password are not accepted.

If you have connected to the board but it does not accept your logon name and password, you must verify that your logon information is correctly configured. Connect to the Remote Insight Lights-Out Edition board using your browser, log on with a user name that has supervisor access, and then re-enter the logon name and password that are not being accepted.

You can also re-enter the logon name and password using the System Configuration Utility. Follow these steps:

1. On the server, run the System Configuration Utility by pressing the **F10** key during power up.
2. Select **Configure Hardware**.
3. Select **Review or Modify Hardware Settings.**
4. Select **View or Edit Details,** and then press **Enter.**
5. Move the cursor down to the Configure Users field, and then press **Enter.**
6. Select the user experiencing a problem, and then verify the logon name. The user's password is not visible, but can be re-entered on this screen.
7. Check the Login Access field on this screen to make sure that this user has logon access.

I have forgotten my administrator password.

If you have forgotten the administrator password for the Remote Insight Lights-Out Edition board, the password can be changed by performing the following steps:

1. Insert the Offline Configuration Data Diskette in the diskette drive of the server.
2. Open the CPQRIB file on the diskette using a text editor.
3. Modify the contents of the file in the password section to reflect the new password.

NOTE: The server automatically updates the password when the server accesses the diskette during its normal polling sequence. This update occurs every five minutes.

I cannot connect to the board through the NIC.

If you cannot connect to the board through the NIC, try any or all of the following troubleshooting methods:

- Confirm that the green LED (link status) on the board connector bracket is illuminated. The LED indicates a good connection between the PCI NIC and the network hub.
- Look for intermittent flashes of the green LED. The LED indicates normal network traffic.
- Run the System Configuration Utility to confirm that the NIC is enabled, and verify the assigned IP address and subnet mask.
- From another workstation on the same network, ping the IP address of the NIC.
- Attempt to connect with browser software by typing the IP address of the NIC as the URL. You can see the Remote Insight home page from this address.
- Reset the Remote Insight Lights-Out Edition board.
- Verify that you are using a valid user name and password.

To reset the Remote Insight Lights-Out Edition board, follow these steps:

1. Right-click the **My Computer** icon of your desktop, and then select **Manage.**
2. Expand the **Services and Applications** folder.
3. Select **Services.**
4. Stop the Compaq Server Agents service. This action stops the Compaq Remote Insight Board Configuration agent, the Compaq Web Agent, and the Compaq Foundation Agents.
5. In Control Panel, select the **Compaq Management Agents** applet.
6. Select the **Remote Insight** tab, and then click the **Reset Remote Insight Board** button.
7. Restart the Compaq Server Agents service.

I cannot get SNMP information from Compaq Insight Manager when connected to the Remote Insight Lights-Out Edition board network interface.

The agents running on the managed server provide the SNMP information provided to Compaq Insight Manager. For those agents to pass information through the Remote Insight Lights-Out Edition board, the Remote Insight Lights-Out Edition board drivers must be installed. See the Remote Insight Light-Out Edition User Guide for installation instructions. .

If you have installed the drivers and agents, and if you are using the Remote Insight Lights-Out Edition board, verify that the Remote Insight Lights-Out Edition board and the management PC are on the same subnet. The subnet can be quickly verified by pinging the Remote Insight Lights-Out Edition board from your management PC. See your network administrator for proper routes to access the Remote Insight Lights-Out Edition board network interface

Web browser does not connect to the Remote Insight Lights-Out Edition board IP address.

If your Web browser software is configured to use a proxy server, the browser does not connect to the Remote Insight Lights-Out Edition board IP address. To resolve this issue, configure your browser to not use the proxy server for the IP address of the Remote Insight Lights-Out Edition board. For example, in Internet Explorer, click **View,** then click **Options,** then **Connection,** then **Settings,** and then enter the IP address under Exceptions.

Troubleshooting Alert and Trap Problems

I am unable to receive Compaq Insight Manager alarms (SNMP traps) from the Remote Insight Lights-Out Edition board.

A user with supervisor access must connect to the Remote Insight Lights-Out Edition board or run the System Configuration Utility to configure SNMP trap parameters.

1. Make sure the correct alert types are enabled, either in the Manage Alert Information screen of the Remote Insight Lights-Out Edition board console application or in the Alerts Received field on the user information screen in the System Configuration Utility.
2. On the server, run the System Configuration Utility and verify that the Alerts field is set to Enabled. This field globally enables or disables alerts for all Remote Insight Lights-Out Edition board users.
3. Verify that the community string and SNMP trap destination is set correctly on the TaskSmart N2400 SNMP service properties.

Miscellaneous Remote Insight Lights-Out Edition Board Troubleshooting

The time or date of the entries in the Event Log are incorrect.

You can update the time and date on the Remote Insight Lights-Out Edition board by running the System Configuration Utility. This utility automatically sets the time and date on the board using the server time and date. Compaq Management Agents for Servers on supported network operating systems also updates the time and date.

How do you interpret LED error codes?

The LED indicators on the front of the Remote Insight Lights-Out Edition board (with the LEDs on top) have the following assignments:

FB	7	6	5	4	3	2	1	0

During the initial start of the Remote Insight Lights-Out Edition board the LED indicators flash randomly. After the Remote Insight Lights-Out Edition board is started, the FB LED flashes once a second. The LED indicators (1 through 7) light after start-up to indicate a hardware failure. If a hardware failure is detected, try resetting the Remote Insight Lights-Out Edition board. Refer to the *Remote Insight Manager Lights-Out Edition User Guide* for more information.

Keyboard and mouse do not work for Remote Console to the Remote Insight Lights-Out Edition board.

Verify that the keyboard and mouse cables on the Remote Insight Lights-Out Edition board are properly installed. (Refer to the *Remote Insight Manager Lights-Out Edition User Guide* for more information on connecting the keyboard cable.)

How do I manage the TaskSmart N2400 appliance from Hewlett Packard OpenView?

Verify that Compaq Insight Manager for Hewlett Packard (HP) OpenView has been installed on your management server. Insight Manager for HP OpenView can be downloaded from the management section of the Compaq website:

http://www.compaq.com/manage

QuickRestore

The TaskSmart N2400 appliance ships with a QuickRestore CD that enables a customer to restore a system to the factory state. Factory state can include or exclude the contents of the attached storage. This section outlines the QuickRestore functionality and the resulting actions a user should take upon completion of the QuickRestore. Please note that some of this information is duplicated in the QuickRestore CD guide included with the QuickRestore CD.

TaskSmart N2400 Appliance Verification

When the QuickRestore CD is loaded into the CD-ROM drive bay and the system unit is powered up, the QuickRestore CD launches and verifies that the CD is placed into a TaskSmart N2400 appliance. If the program detects a noncertified TaskSmart N2400 system, a warning message is displayed and the QuickRestore process is exited.

QuickRestore Options

After the QuickRestore CD loads, the following menu options are presented:

- **OS Restore—**Restores NAS operating system only and leaves data drives untouched
- **Full Restore—**Restores NAS operating system and data drives back to factory state
- **Help—**Provides information about the QuickRestore CD
- **Exit—**Exits the QuickRestore CD and restarts the system

Selecting the Full Menu Option

If the Full menu option is selected, a warning message that all data is about to be deleted is displayed. The restore process does not continue until confirmation that user wishes to erase the entire system is indicated by selecting yes or no.

After system configuration has completed, the user is presented with the following menu to restore and configure the external data drives:

- **Manual—**QuickRestore does not attempt to configure the external storage. External storage is left unconfigured. Refer to the “Storage Management” section in Chapter 4, “Integrating UNIX into Windows NT.”
- **Automatic—**QuickRestore automatically configures the drives based on the factory carving in Table C-6. Note the number of drives included in the external storage cabinet determines the number of arrays to be carved. Storage configuration also includes the creation of pools and virtual disks that are associated with the Compaq Virtual Replicator software on the TaskSmart N2400 appliance.

The data drives are segregated into groups of disks no larger than 14 and no smaller than 4. Each of these groups of disks are treated as RAID 5 arrays.

Table C-8
Data Drive Groups

Number of Storage Enclosures	Number of Drives	Drives Lost to RAID 5 Arrays	Number of RAID 5 Arrays
1	4 to 14	1	1
2	15 to 28	2	2
3	29 to 42	3	3
4	43 to 56	4	4

For each created RAID set, a single logical drive, pool, and virtual disk are created.

NOTE: The TaskSmart N2400 appliance supports spare drives (or set of spare drives) for the collective storage subsystem. QuickRestore does not have the ability to interactively determine the use of spares.

Configuring Spares

For spare drives, the user should set aside the appropriate number of desired spares before starting QuickRestore. Upon completion of QuickRestore and final setup, the user must:

1. Power down the server.
2. Add the spare drive or drives.
3. Power up the system.
4. Assign the spare drives manually to the arrays as spares through the Array Configuration Utility.

QuickRestore Menu Option

If the QuickRestore menu option is selected, the QuickRestore CD performs the following tasks:

1. Launches the configuration utility and configures the unit as it arrived from the factory. If options are added and recognized by the configuration utility, they are automatically included.
2. Erases the operating system disks inside the server bays and reconfigures them to the factory default state.
3. Restarts the system.
4. Launches the Compaq Imaging processes and, upon completion, restarts the system.
5. Automatically ejects the QuickRestore CD, marking the completion of the QuickRestore process.
6. Restarts the system a final time.

Full Restore Menu Option

If the Full Restore menu option is selected, the QuickRestore CD performs the following tasks:

1. Selects the desired external storage configuration option. For more information about this selection, see the *TaskSmart N2400 QuickRestore CD Guide* included with the QuickRestore CD.
2. Erases the operating system drives inside the server bays and external storage.

IMPORTANT: A manual restart of the system is required to continue.

3. Launches the configuration utility and configures the system to factory default settings. If options are added and recognized by the configuration utility, they are automatically included.
4. Configures the operating system drives inside the server bays to factory default state.
5. Configures the external storage drives to the desired option specified in step 1.
6. Restarts the system for the configuration changes to take effect.
7. Launches the Compaq Imaging process and, upon completion, restarts the system.
8. Automatically ejects the QuickRestore CD, marking the completion of the QuickRestore process.
9. Restarts the system.

Post QuickRestore and Automated Setup

Upon completion of the restoration, the system is configured as it came from the factory. The user should follow the same steps of initial setup that were followed during the initial configuration. Initial setup is identified by two major phases. These include:

- The Microsoft Setup interviews
- The TaskSmart Setup utilities

Each of these phases is intended to be fully automated if the configuration diskette, produced by the Offline Configuration tool, is present in the diskette drive.

△ **CAUTION:** During the setup process, several Microsoft setup screens are displayed. The user must not interact with the interface that is presented. If the setup process stops during the Microsoft setup interview for more than 15 minutes, the configuration file can become corrupted or altered in some way. Power down at the Microsoft setup phase to allow the unit to restart the setup phase.

Post QuickRestore Additional Setup

Upon completion of the setup of the server, tasks must be performed to return the TaskSmart N2400 appliance to the previous state (before the QuickRestore process) unless a factory state is desired. These tasks can include:

- Reset the system date, time, and time zone.
- Reinstall third-party backup software.
- Add the TaskSmart N2400 appliance into the domain that it was originally a part of.
- Re-establish user accounts, if the TaskSmart is a part of a workgroup.
- Re-establish user rights to drives, files, and directories, if the files were retained.

  NOTE: Being a part of a domain negates this requirement.

- Restore data from tape to the external storage cabinets.
- Restore data from tape to the operating system disk drives.

In general, the steps for a full recovery of a system from a failed state, provided in Appendix A, “Backup Utility Management,” may be required if the QuickRestore CD is used.

Miscellaneous Troubleshooting

Incorrect ROM

The server indicates an incorrect ROM and then a blue screen error is displayed, with the following codes: 0x1E: 0x61736B, 0x536D6172, 0x74204241, 0x44524F4D.

The software runs only on the TaskSmart N2400 appliance. Contact Compaq technical support.

System Event Log

My system event log contains entries that state that a particular pool has less than 30 percent space available.

Either delete old snapshots or add more storage capacity. Add more storage to the server by adding additional hard drives, external storage systems, or both. See Chapter 4, “Integrating UNIX into Windows NT,” for capacity expansion information.

External Storage System

The external storage system is reporting a power supply failure.

This can be caused by a loss of power from the power source connected to the power supply, or it can be caused by a power supply failure. Verify that the power supply is connected and plugged in. If the power supply itself has failed, **leave it in place.** The remaining fan is capable of providing adequate cooling to the external storage system, as long as the failed module is still installed. Contact Compaq technical support for replacement of the failed power supply, and when the replacement is received, replace the failed power supply with the new one. **It is not necessary to power down your server or your external storage system.**

Compaq Insight Manager

Compaq Insight Manager notifies me of an impending failure of a hard drive, memory module, or processor.

Contact Compaq technical support to get a replacement hard drive, memory module, or processor under the Compaq Pre-Failure Warranty. When the new part arrives, replace it. Note that hard drives can be replaced without server or external storage system or systems being powered down. Processor and memory replacement require that the server be powered down. Ask your Compaq authorized service provider for details if in doubt.

Appendix D

Regulatory Compliance Notices

Regulatory Compliance Identification Numbers

For the purpose of regulatory compliance certifications and identification, the server and storage enclosure of the Compaq TaskSmart N2400 appliance are each assigned a Compaq series number. The Compaq series number for the server is ES1009 and the series number for the storage enclosure is EK1502. The TaskSmart N2400 appliance server and storage enclosure series numbers can be found on their respective product labels, along with the required approval markings and information. When requesting certification information for these products, always refer to the series numbers. These series numbers must not be confused with the marketing name or model number for your Compaq TaskSmart N2400 appliance.

Federal Communications Commission Notice

Part 15 of the Federal Communications Commission (FCC) Rules and Regulations has established Radio Frequency (RF) emission limits to provide an interference-free radio frequency spectrum. Many electronic devices, including computers, generate RF energy incidental to their intended function and are, therefore, covered by these rules. These rules place computers and related peripheral devices into two classes, A and B, depending upon their intended installation. Class A devices are those that may reasonably be expected to be installed in a business or commercial environment. Class B devices are those that may reasonably be expected to be installed in a residential environment (for example, personal computers). The FCC requires devices in both classes to bear a label indicating the interference potential of the device as well as additional operating instructions for the user.

The rating label on the device shows the classification (A or B) of the equipment. Class B devices have an FCC logo or FCC ID on the label. Class A devices do not have an FCC logo or ID on the label. After the class of the device is determined, refer to the corresponding statement in the following sections.

Class A Equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at personal expense.

Class B Equipment

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit that is different from that to which the receiver is connected
- Consult the dealer or an experienced radio or television technician for help

Declaration of Conformity for Products Marked with the FCC Logo—United States Only

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For questions regarding your product, contact:

Compaq Computer Corporation
P. O. Box 692000, Mail Stop 530113
Houston, Texas 77269-2000

Or call 1-800-652-6672 (1-800-OK COMPAQ). For continuous quality improvement, calls may be recorded or monitored.

For questions regarding this FCC declaration, contact:

Compaq Computer Corporation
P. O. Box 692000, Mail Stop 510101
Houston, Texas 77269-2000

Or call 281-514-3333.

To identify this product, refer to the part, series, or model number found on the product.

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Compaq Computer Corporation may void the user’s authority to operate the equipment.

Cables

Connections to this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

Canadian Notice (Avis Canadien)

Class A Equipment

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Class B Equipment

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Mouse Compliance Statement

This mouse complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

European Union Notice

Products with the CE Marking comply with both the EMC Directive (89/336/EEC) and the Low - Voltage Directive (73/23/EEC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms (the equivalent international standards are in parentheses):

- EN55022 (CISPR 22)—Electromagnetic Interference
- EN50082-1 (IEC801-2, IEC801-3, IEC801-4)—Electromagnetic Immunity
- EN60950 (IEC950)—Product Safety

Japanese Notice

ご使用になっている装置にVCCIマークが付いていましたら、次の説明文をお読み下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

VCCIマークが付いていない場合には、次の点にご注意下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です　この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Taiwanese Notice

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Laser Devices

All Compaq systems equipped with a laser device comply with safety standards, including International Electrotechnical Commission (IEC) 825. With specific regard to the laser, the equipment complies with laser product performance standards set by government agencies as a Class 1 laser product. The product does not emit hazardous light; the beam is totally enclosed during all modes of customer operation and maintenance.

Laser Safety Warnings

WARNING: To reduce the risk of exposure to hazardous radiation:

- Do not try to open the laser device enclosure. There are no user-serviceable components inside.
- Do not operate controls, make adjustments, or perform procedures to the laser device other than those specified herein.
- Allow only Compaq authorized service technicians to repair the laser device.

Compliance with CDRH Regulations

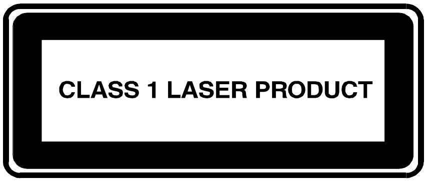
The Center for Devices and Radiological Health (CDRH) of the U.S. Food and Drug Administration implemented regulations for laser products on August 2, 1976. These regulations apply to laser products manufactured from August 1, 1976. Compliance is mandatory for products marketed in the United States.

Compliance with International Regulations

All Compaq systems equipped with laser devices comply with appropriate safety standards including IEC 825.

Laser Product Label

The following label or equivalent is located on the surface of the laser device supplied by Compaq.



This label indicates that the product is classified as a CLASS 1 LASER PRODUCT. This label is affixed to a laser device installed in your product.

Laser Information

The following list describes standard laser specifications:

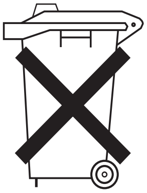
Laser type	Semiconductor GaAIAs
Wave length	780 nm +/- 35 nm
Divergence angle	53.5 degrees +/- 0.5 degrees
Output power	Less than 0.2 mW or 10,869 W·m-2 sr-1
Polarization	Circular 0.25
Numerical aperture	0.45 inches +/- 0.04 inches

Battery Replacement Notice

Your computer is equipped with a lithium manganese dioxide, a vanadium pentoxide, or an alkaline internal battery or battery pack. There is a danger of explosion and risk of personal injury if the battery is incorrectly replaced or mistreated. Replacement is to be done by a Compaq authorized service provider using the Compaq spare designated for this product. For more information about battery replacement or proper disposal, contact your Compaq authorized reseller or your authorized service provider.

⚠ **WARNING:** Your computer contains an internal lithium manganese dioxide, a vanadium pentoxide, or an alkaline battery pack. There is risk of fire and burns if the battery pack is not handled properly. To reduce the risk of personal injury:

- Do not attempt to recharge the battery.
- Do not expose to temperatures higher than 60°C.
- Do not disassemble, crush, puncture, short external contacts, or dispose of in fire or water.
- Replace only with the Compaq spare designated for this product.



Batteries, battery packs, and accumulators must not be disposed of together with the general household waste. To forward them to recycling or proper disposal, please use the public collection system or return them to Compaq, your authorized Compaq Partners, or their agents.

Appendix E

Electrostatic Discharge

A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the Compaq TaskSmart N2400 appliance.

To prevent electrostatic damage, observe the following precautions:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded (earthed) surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always be properly grounded when touching a static-sensitive component or assembly.

Grounding Methods

There are several methods for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded (earthed) workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm ± 10 percent resistance in the grounding cords. To provide proper grounding, wear the strap snug against the skin.
- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have a Compaq authorized reseller install the part.

NOTE: For more information on static electricity, or assistance with product installation, contact your Compaq authorized reseller.

Index

A

Access Control List *See* ACL
Access Control Settings
  Auditing tab dialog box for folder name NTSF Test, illustrated 3-65
  dialog box for folder name NTSF Test Permissions tab, illustrated 3-62
  Owner tab dialog box for folder name NTSF Test, illustrated 3-68
Access Control Settings, advanced
  adding user or group 3-64
  auditing tab 3-65
  Owner tab 3-68
  permissions tab 3-61
  removing user or group 3-64
Account Information dialog box, illustrated 3-48
ACL (Access Control List)
  access level permissions 3-57
  access levels 3-58
  defined 1-14
  described 3-55
  permission levels 3-55
  security, integrating 3-69
  user and group access 3-55
Active Directory
  account properties 3-29
  Builtin folder 3-21
  contents 3-21
  creating
    new group 3-36
    user 3-22
  creating a password 3-23
  creating an account 3-21
  deleting a user 3-26
  deploying under Windows 2000 3-36
  domain controller, functions 3-15
  domain environment, described 3-15
  managing user accounts 3-30
  modifying a user 3-27, 3-33
  passwords 3-41
  placing appliance into 3-41
  primary group 3-34
  profile properties 3-31
  properties
    member of 3-33
    modifying 3-28
  registering appliance 3-41
  sessions properties 3-34
ActiveAnswers
  help, Active Directory 3-21
  website 3-15, 3-21, 3-36

- ACU (Array Configuration Utility)
  - accessing C-12, C-13
  - configuration wizard, bypassing 6-36
  - configuring the array controller B-4
  - creating logical drives 6-12
  - data destructive operation B-4
  - defined C-12
  - features 6-4
  - graphical configuration utility B-4
  - managing drive arrays 6-7
  - storage management 6-4
  - System Configuration menu C-12
  - wizards 6-4
- adaptive load balancing *See* ALB
- Add Computer to Domain dialog box, illustrated 3-39
- Add Standalone Snap-in dialog box, illustrated 3-17
- Add Users and Groups dialog box, illustrated 3-50
- addressing server failures 4-27
- administrative procedures, listed 2-1
- ADU (Array Diagnostic Utility)
  - accessing C-12
  - defined C-12
  - described C-18
  - drive failure 6-27
  - interruption, caution C-18
  - starting C-18
- advanced maps for NIS
  - Show User Maps dialog box, illustrated 4-22
- advanced maps for PCNF, Show User Maps dialog box, illustrated 4-20
- Advanced Server Logical Volume Manager *See* LVM
- ALB (adaptive load balancing)
  - defined 6-46
  - teaming option, Cisco Fast EtherChannel 6-46
  - using 6-46
- array accelerator, battery backup 6-7
- Array Configuration Utility *See* ACU
- array controller
  - configuring B-4
  - firmware 6-26
  - moving drives 6-26
- Array Diagnostic Utility *See* ADU
- arrays
  - capacity expansion 6-35
  - creating 6-7
  - moving 6-34
  - moving drives
    - conditions 6-26
    - steps 6-26
- ASR-2 (Automatic Server Recovery-2)
  - allowing network access C-28
  - attended recovery C-23
  - configuring C-22
  - default value C-26
  - description C-22
  - flowchart C-27
  - flowcharts C-27
  - illustrated C-27
  - offsite servers C-26
  - paging administrator C-22
  - remote servers C-26
  - software error
    - recovery C-25
    - recovery start option C-25
    - recovery timeout C-25
  - standby recovery
    - server option C-25
    - server port C-25
    - time out C-25

- starting into Compaq Utilities C-28
- starting into operating system C-29
- thermal shutdown C-25
- timer C-26
- unattended recovery C-23
- UPS
  - shutdown C-25
  - shutdown threshold C-25

Auditing Entry dialog box for folder NTSF Test, illustrated 3-67
automatic data recovery 6-32
Automatic Server Recovery-2 *See* ASR-2

B

backup and restoration of mappings 4-26
backup domain controller *See* BDC
backup procedures
- caution 2-19

backup software
- trial versions A-5
- vendor capabilities, listed A-5

backup solutions
- archive setup information A-6
- automatic backup schedules A-7
- catastrophic failures, listed A-7
- considerations A-2
- developing A-2
- disaster recovery A-9
- Fibre Channel A-4
- media rotation A-8
- multiple backup devices A-8
- offsite storage A-1, A-8
- readiness testing A-8
- regular backups A-6
- SCSI
  - direct-connect A-3
  - implementing A-3
- software vendors A-5
- tape devices
  - connection methods A-3
  - described A-2
  - FC-AL A-4
  - Fibre Channel A-4
  - hardware compatibility A-4
  - SCSI connections A-3
  - SCSI, direct connect A-3
  - switched Fibre Channel A-4

backup tools
- considerations A-2
- sizing
  - described A-2
  - direct connection A-2
  - enterprise solutions white paper A-2
  - fibre connection A-2
- website resources A-2

batteries
- replacement notice D-8
- warning D-8

battery
- backup
  - array accelerator 6-7
  - data integrity 6-7
- charge time 6-7
- recycling or disposal D-8

BDC (backup domain controller)
- defined 4-12
- password synchronization 6-62

Builtin folder, Active Directory 3-21

C

- caching
  - setting through Windows Explorer 3-85
  - settings, listed 3-80
- Caching Settings dialog box, illustrated 3-80
- Canadian Notice
  - Class A equipment D-4
  - Class B equipment D-4
- capacity expansion
  - configuration 6-35
  - features 6-35
  - procedure 6-35, 6-36
- cautions
  - ADU, interruption C-18
  - avoiding configuration damage 1-12
  - backup procedures 2-19
  - CIFS sessions, disconnecting 3-82
  - corrupted configuration file C-56
  - data backup 6-26
  - data corruption 2-30
  - data loss C-6
  - defined x
  - drive bays 6-31
  - drive defragmentation 2-26
  - fault tolerance, RAID C-6
  - hard drives
    - replacing 6-34
    - replacing 6-28
  - hard drives, replacing 6-29
  - hot-plug hard drive, replacement C-5, C-7
  - Lifeguard, using during restore 2-29
  - logical drives
    - extending 6-2
  - logical drives 6-14, 6-22
    - deleting 6-10
  - loss of fault tolerance C-4
  - LVM 6-14
  - open files, disconnecting 3-83
  - snapshot recovery 2-20
  - snapshots 2-29
- CDRH (Center for Devices and Radiological Health), compliance D-6
- CE Marking D-5
- Center for Devices and Radiological Health *See* CDRH
- Change permission level 3-77
- CIFS (Common Internet File System)
  - closing a single open file 3-83
  - closing all open files 3-83
  - compatibility with NFS 3-88
  - defined 1-14
  - described 3-1
  - disconnecting session 3-82
  - domain environment
    - administering users and groups 3-15
    - described 3-15
  - domain environments 3-1
  - environments
    - compared 3-2
    - users and groups 3-1
  - home directory 3-47
  - managing sessions with MMC 3-82
  - open file management 3-83
  - setting caching through Windows Explorer 3-85
  - setting permissions through Windows Explorer 3-85
  - shares
    - accessing 3-1
  - terminating session 3-82
  - workgroup environments 3-1
- CIFS (Common Internet File System) sessions, disconnecting caution 3-82
- CIFS (Common Internet File System) shares 3-70

  - administering through Windows Explorer 3-84
  - administrative and standard 3-88
  - creating
    - methods 3-70
    - with command line 3-70
    - with MMC 3-72
  - deleting through Windows Explorer 3-86
  - modifying through Windows Explorer 3-87
  - NET SHARE command 3-70
  - setting up through Windows Explorer 3-84
- Cisco Fast EtherChannel *See* FEC
- client groups
  - illustrated 4-30
  - NFS, defined 4-30
- command line
  - capabilities 4-32
  - management utility, described 2-7
  - NFS, stopping and starting C-37
- Command line interface, illustrated 4-32
- Command Prompt screen, illustrated 2-7
- Common Internet File System *See* CIFS. *See* CIFS. *See* CIFS
- communication parameters, setting C-28
- Compaq authorized reseller xiii
- Compaq Diagnostics
  - accessing C-12
  - defined C-14
- Compaq Insight Manager
  - Agent Web interface 5-11
  - Agent Web interface, illustrated 5-11
  - components 5-9
  - console Web browser 5-10
  - described C-19
  - detecting drive failure 6-27
  - discover IP devices 5-10
  - installing management software 5-15
  - management agents
    - network interface 5-9
    - storage subsystem performance 5-9
  - remote administration 5-9
  - viewing the event list C-20
- Compaq Insight Manager for HP OpenView
  - remote administration 5-12
- Compaq Insight Manager for Tivoli NetView (AIX), Version 2.0
  - remote administration 5-14
- Compaq Integrated Remote Console, features C-26
- Compaq Management Agents for Servers, enabling C-21
- Compaq Network Teaming and Configuration *See* CPQTEAM
- Compaq Network Teaming and Configuration Properties dialog box, illustrated 6-43
- Compaq Pre-Failure Warranty
  - Smart Array Controller 6-6
- Compaq Series Number, regulatory compliance D-1
- Compaq Survey Utility, viewing C-20
- Compaq system partition, accessing utilities C-12
- Compaq telephone numbers xiii
- Compaq website xii, xiii
- compatibility, NFS and CIFS 3-88
- configuration
  - all environments 1-13
  - changing storage management settings 1-15
  - Configuration Utility CD
    - described 1-4
    - inserting 1-5
  - creating the data diskette 1-4
  - damage, caution 1-12
  - optional tasks 1-15
  - passwords 3-5

- UNIX and Windows NT multiprotocol environment 1-14
- warning screen, illustrated 1-11
- Windows NT workgroup and domain security
  - environment 1-14
  - environment, CIFS sharing 1-14
- Windows NT/UNIX
  - CIFS sharing 1-14
  - NFS sharing 1-15
  - UNIX to Windows NT user mapping 1-14
- wizard-style interface 1-5

configuration data diskette
- inserting into the diskette drive, illustrated 1-7

configuration data diskette, inserting into the diskette drive, illustrated 1-4

Configuration Utility CD
- inserting into the CD-ROM drive, illustrated 1-5

console screen, illustrated 6-8

Correctable Memory Logs *See* IML

corrupted configuration file
- caution C-56

CPQTEAM (Compaq Network Teaming and Configuration
- Ethernet Teaming 6-37

CPQTEAM (Compaq Network Teaming and Configuration)
- adding NIC to team 6-41
- opening 6-40
- teaming option
  - fault tolerance 6-44
  - load balancing 6-46

CPQTEAM (Compaq Network Teaming and Configuration) Properties screen Diagnostic tab, illustrated C-42

CPQTEAM (Compaq Network Teaming and Configuration) Properties screen, Diagnostic tab test results, illustrated C-43

CPQTEAM (Compaq Network Teaming and Configuration) Properties screen, illustrated C-41

CPQTEAM (Compaq Network Teaming and Configuration) Utility
- installing 6-38

Create Drive Array A screen, illustrated 6-11

Create Logical Drive dialog box, illustrated 6-13

Create Shared Folder dialog box
- customizing, illustrated 3-75

Create Shared Folder dialog box, illustrated 3-74

Create Snapshot Wizard screen, illustrated 2-28

cross-platform share management, requirements 3-88

Customize Permissions dialog box
- Security tab, illustrated 3-78
- Share Permissions tab, illustrated 3-76

D

data backup, caution 6-26

data corruption, caution 2-30

data guarding *See* RAID 4

data loss
- caution C-6

data striping *See* RAID 10

date, time, and time zone, changing 1-13

default configuration, unique to TaskSmart N2400 appliance C-10

device information window, illustrated 5-10

DHCP (dynamic host configuration protocol) 5-4
  defined 1-3
diagnosing problems
  hard drives C-5
  network interface controllers (NICs) C-38, C-40, C-42
  NICs C-38, C-41, C-43, C-44
diagnosing problems, hard drives C-6
diagnostic tools
  accessing C-12
  diskette, creating C-14
  error codes C-14
  running C-15
  starting remotely C-28
  test error codes, description C-14
Diagnostics *See* Compaq Diagnostics
Diagnostics and Utilities menu
  Inspect Computer C-14
  Remote Utilities C-14
  Test Computer C-14
  Upgrade Firmware C-14
disaster recovery
  backup solutions A-9
  steps A-9
diskette drive, disabling C-30
diskette, creating diagnostics C-14
distributed data guarding *See* RAID 5
DNS (domain name system) 5-4
domain and workgroup environments, compared 3-2
domain controller
  administering users and groups
    from console 3-16
    remotely 3-16
  functions 3-15
domain environment
  compared to workgroup 3-2
  domain controller 3-15
  Server Manager
    user account
      characteristics 3-44
  User Manager for Domains 3-43
domain environment, Active Directory
  account properties 3-29
  adding TaskSmart N2400 appliance 3-19
  adding to account 3-19
  Builtin folder 3-21
  creating a new group 3-36
  creating a password 3-23
  creating an account 3-21
  creating user 3-22
  deleting a user 3-26
  managing user accounts 3-30
  member properties 3-33
  modifying a user 3-27, 3-33
  passwords 3-41
  placing appliance into 3-41
  primary group 3-34
  profile properties 3-31
  properties, modifying 3-28
  registering appliance 3-41
  sessions properties 3-34
  user name 3-41
domain environment, Server Manager 3-37
  account properties 3-48
  adding a user 3-44
  administering users and groups 3-43
  creating an account 3-39
  creating new global group 3-51
  deleting a user 3-49
  described 3-37
  launching 3-37
  logon access 3-48
  modifying a user profile 3-47
  modifying a username 3-49

- modifying group 3-51
- modifying group memberships 3-46
- modifying user properties 3-49
- User Manager 3-49

Domain Username and Password dialog box, illustrated 3-41
domains, multiple 4-26
drive arrays
- managing, ACU 6-7

drive bays
- caution 6-31

drive defragmentation, caution 2-26
drive failure
- ADU 6-27
- backups 6-33
- fault tolerance 6-33
- hot spare drives 6-32
- LED status indicators 6-27
- moving arrays 6-34
- online spare drives 6-32
- POST message 6-27
- recognizing 6-27
- replacing failed drive 6-27
- spare drives 6-32

drive mirroring *See* RAID 1
drive quotas *See* quotas
dynamic host configuration protocol *See* DHCP

E

ECC (error checking and correcting)
- defined 6-6

electric shock
- warning x, xi

electric shock hazards symbol x
electrostatic discharge *See* ESD
Enable Drive A, Boot, option 2-9
enterprise management
- Compaq Insight Manager for HP OpenView 5-12
- Compaq Insight Manager for Tivoli NetView (AIX), Version 2.0 5-14
- HP OpenView 5-12
- remote administration 5-12
- Tivoli NetView (Linux) 5-14

environmental recovery C-22
environments
- domain 3-1
- workgroup 3-1

error checking and correcting *See* ECC
error codes
- 100 through 199 C-16
- diagnostic C-14

error condition, resolving C-15
ESD (electrostatic discharge)
- damage caused by E-1
- obtaining additional information E-2
- parts handling E-1
- parts transporting E-1
- precautions E-1
- preventing E-1

Ethernet connectors
- described 1-8
- server, illustrated 1-8

Ethernet ports
- configuring 1-3
- loopback cables 1-9
- usage 1-8

Ethernet Teaming
- CPQTEAM 6-37
- features 6-37
- procedures 6-37

European Union Notice D-5
Event List
- described C-21
- printing C-20
- viewing C-20

exclamation point symbol x
exporting files
  heterogeneous
    environment 4-9
  homogeneous
    environment 4-9

F

failure condition recovery, hard drives C-4, C-5, C-6, C-7
failures, catastrophic A-7
fault tolerance C-5
  compromised 6-33
  configuring teams, help 6-45
  data loss 6-33
  increasing 6-37
  loss of, caution C-4
  nondrive problems 6-33
  RAID 0 B-3
  RAID 1 B-3
  RAID 10 B-3
  RAID 4 B-1
  RAID 5 B-1
  RAID, caution C-6
  teaming option
    fail on fault 6-44
    manual 6-44
    smart switch 6-45
FC-AL (Fibre-Channel Arbitrated Loop)
  defined A-4
  tape libraries A-4
FCC (Federal Communications Commission
  notice D-2
FCC (Federal Communications Commission)
  cables D-3
  Class A equipment compliance
    notice D-2
  Class B equipment compliance
    notice D-2
  Declaration of
    Conformity D-3
  modifications D-3
  mouse compliance
    statement D-4
FEC (Fast EtherChannel)
  defined 6-46
  teaming 6-46
Federal Communications Commission *See* FCC
Fibre Channel
  backup solutions, tape
    devices A-4
  environments
    FC-AL A-4
    switched A-4
    types A-4
Fibre-Channel Arbitrated Loop *See* FC-AL
file exporting
  capabilities 4-28
  NFS 4-28
  snap-ins, listed 2-5
file locking, NFS 4-31
file management, described 3-83
file system security, managing with the Remote Insight Lights-Out Edition board 3-60
flowchart, ASR-2 C-27
flowcharts
  ASR-2 C-27
front bezel
  removing 1-6
  removing, illustrated 1-6
Full Control permission level 3-77

G

getting help xii
GID (group ID)
    authentication 4-5
    defined 1-14
Global Group Properties dialog box, illustrated 3-53
Global Unique Identifier *See* GUID
graphics, disabling on-board C-30
grounding methods E-2
group ID *See* GID
Group ID *See* GID
Group Memberships dialog box, illustrated 3-46
Guests Properties, dialog box, illustrated 3-14
GUID (Global Unique Identifier), defined 4-9

H

hard drive LEDs
    activity
        combination functions 6-29
    fault
        combination functions 6-29
    online
        combination functions 6-29
hard drives 6-29
    failure, lost data 6-34
    failure, POST C-3
    fault tolerance 6-33, C-5
    hot-plug guidelines C-4, C-5, C-6, C-7
    LED indicators 6-28
    LEDs
        activity 6-29, 6-30
        combinations 6-29
        fault 6-29, 6-30
        online 6-29, 6-30
    mirrored pairs C-5
    moving, steps 6-26
    online spare C-5
    predictive failure replacement guidelines C-6
    recognition C-4
    replacing 6-27, 6-31, 6-33
    replacing, caution 6-28, 6-29, 6-34
    server does not recognize C-3
    troubleshooting C-2, C-3, C-8
hardware issues *See* technical support
hazard symbol x
hazardous energy circuits symbol x
Health Driver, description C-26
help
    Active Directory, ActiveAnswers website 3-21
    ActiveAnswers website 3-21
    additional help, listed 2-10
    backup tools website A-2
    Compaq authorized reseller, telephone numbers xiii
    Compaq technical support xii
    Compaq website xiii
    groups, use of 3-21
    Insight Manager for Tivoli (AIX), website 5-15
    locations described xii
    Windows file system security website 3-55
Help
    dialog box, illustrated 2-10
    icon 2-10
High Voltage Differential *See* HVD
host configuration protocols, DHCP and non-DHCP 1-3
hot surface, warning xi
hot surfaces symbol xi
hot-plug drives *See* hard drives
hot-plug hard drive
    LEDs, illustrated 6-28
    replacement, caution C-5, C-7

hot-plug hard drives
    device problems C-8
hot-pluggable drives *See* hard drives
HP OpenView
    Network Node Manager 5-13
    remote administration 5-9
    Windows 2000 operating system 5-12
HVD (High Voltage Differential)
    defined A-4

I

ID positions, altering 6-26
Identification Changes dialog box, illustrated 3-40
illustrations
    Access Control Settings
        Auditing tab dialog box for folder name NTSF Test 3-65
        dialog box for folder name NTSF Test, Permissions tab 3-62
        Owner tab dialog box for folder name NTSF Test 3-68
    Account Information dialog box 3-48
    Add Computer to Domain dialog box 3-39
    Add Standalone Snap-in dialog box 3-17
    Add Users and Groups dialog box 3-50
    advanced maps for NIS, Show User Maps dialog box 4-22
    advanced maps for PCNF, Show User Maps dialog box 4-20
    ASR-2, flowchart C-27
    Auditing Entry dialog box, for folder name NTSF Test 3-67
    Caching Settings dialog box 3-80
    client groups tab 4-30
Command line interface 4-32
Command Prompt screen 2-7
Compaq Insight Manager, Agent Web interface 5-11
Compaq Network Teaming and Configuration Properties dialog box 6-43
Compaq Network Teaming and Configuration Properties screen C-41
Compaq Network Teaming and Configuration Properties screen Diagnostic tab C-42
Compaq Network Teaming and Configuration Properties screen Diagnostic tab test results C-43
Compaq System Tools menu, selection screen 6-9
configuration data diskette, inserting into the diskette drive 1-4, 1-7
Configuration Utility CD, inserting into the CD-ROM drive 1-5
configuration, warning screen 1-11
console screen 6-8
CPQTEAM dialog box 6-48, 6-55
CPQTEAM installation, complete 6-40
CPQTEAM Restart dialog box 6-49
Create Drive Array A screen 6-11
Create Logical Drive dialog box 6-13
Create Shared Folder dialog box 3-74
Create Shared Folder dialog box, customizing 3-75
Create Snapshot Wizard screen 2-28

- Customize Permissions dialog box
  - Security tab 3-78
- Customize Permissions dialog box, Share Permissions tab 3-76
- device information window 5-10
- distributed data guarding, RAID 5 B-2
- Domain Username and Password dialog box 3-41
- end of the initialization process screen 1-12
- Ethernet connectors, server 1-8
- front bezel, removing 1-6
- Global Group Properties dialog box 3-53
- Group Memberships dialog box 3-46
- Guests Properties, dialog box 3-14
- Help dialog box 2-10
- hot-plug hard drive, LEDs 6-28
- Identification Changes dialog box 3-40
- installing CPQTEAM 6-39
- Internet Protocol (TCP/IP) Properties dialog box 6-41
- launching CPQTEAM setup 6-38
- License Warning dialog box 6-48
- Load Balancing Control teaming 6-46
- Local Area Connection Internet Protocol Properties dialog box 6-53
- Local Area Connection Properties dialog box 6-52, 6-54
- Logoff dialog box 2-8
- map maintenance 4-26
- mapping server ls -al command example 4-11
- Microsoft Management Console screen 2-3
- Modify User Pproperties
  - Member Of tab dialog box 3-33
- Modify User Properties
  - Account tab dialog box 3-29
  - General tab dialog box 3-28
  - Profile tab dialog box 3-32
  - Sessions tab dialog box 3-35
- Modify User Properties, dialog box 3-8
- Network and Dial-up Connections screen 6-50
- Network Identification welcome dialog box 3-42
- Network Properties dialog box 6-51
- New Global Group dialog box 3-51
- New Group, dialog box 3-11
- New Local Group dialog box 3-52
- New Object
  - User dialog box, information summary 3-25
  - User dialog box, password information 3-23
  - User dialog box, user information 3-22
- New Object - Computer dialog box 3-19
- New Object - Group dialog box 3-36
- New Share dialog box 3-85
- New Snapshot Wizard screen 2-18
- New User dialog box
  - User Manager for Domains menu 3-44
- New User, dialog box 3-4
- NFS Server on local computer, Logging tab 4-8
- NFS Server, User Mapping 4-7

NIC Properties dialog box 6-42
NIS configuration screen 4-14
NTFS File Permission Entry, for file name screen 3-56
PCNSF, configuration screen 4-15
Primary User Mapping applied 4-25
RAID 1, drive mirroring, B-4
restart system, dialog box 2-8
Restore From Snapshot Wizard
  Schedule Information dialog box 2-25
  Snapshot Information dialog box 2-22
  Task Information dialog box 2-23
  User Identification for Scheduled Task dialog box 2-24
Security Properties dialog box, for folder name NTSF Test 3-60
Select Domain dialog box, Administering Users and Groups 3-43
Select Domain dialog box, Server Manager 3-38
Select Groups, dialog box 3-10
Select User, Computer, or Group dialog box 3-66
Select Users or Groups, dialog box 3-12
Selected Logical Drives dialog box 6-16
selecting CPQTEAM file path 6-39
server, powering up 1-10
Set Password, dialog box 3-7
set primary user mapping 4-24
SFU file locking 4-31
SFU Password Synchronization dialog box 6-59
SFU Password Synchronization dialog box, advanced settings 6-61
SFU screen user interface 4-1
Share Properties dialog box, General tab 3-79
Shutdown, dialog box 2-9
simple maps for NIS
  Show User Maps dialog box 4-18
simple maps for PCNF
  Show User Maps dialog box 4-16, 4-17
simple maps in mapped users list for NIS dialog box 4-19
SmartArray Controller Configuration Utility, preview dialog box 6-10
Snapshot Manager interface 6-17
Snapshot Manager screen 6-15
  creating snapshots 2-17
  deleting a virtual disk 6-20
  scheduling snapshots 2-27
Snapshot Manager screen, deleting snapshots 6-19
space management process 6-3
TaskSmart N2400 Console 2-2
TaskSmart NAS Management dialog box
  CIFS Session manager using MMC 3-82
  Open Files manger using MMC 3-83
TaskSmart NAS Management MMC consol for file sharing administration 3-73
Teaming Controls dialog box, Fault Tolerant option 6-44
Telnet Server, interface screen 5-2

- User Environment Profile dialog box 3-47
- User Name Mapping user interface 4-10
- User or Group Permission Entry dialog box, for folder name NTSF Test 3-63
- User Properties dialog box, Member Of tab 3-9
- UserData Properties dialog box, Sharing tab 3-84, 3-87
- Web Enabled interface 5-13
- Windows user and UNIX user
  - to map and add for PCNFS dialog box 4-21
- Windows users and UNIX users
  - to map and add for NIS dialog box 4-23

IML (Integrated Management Log)
- Compaq Insight Manager C-19
- described C-19
- error messages C-24
- error types, explained C-24
- recorded information C-24, C-27, C-28, C-29
- security levels C-19
- viewing C-19, C-20, C-24

IML (Integrated Management Log) Event List, described C-21

IML Event List *See also* Event List

Important Safety Information document xi

initialization *See also* initialization tasks
- collect information 1-3
- Configuration Utility CD 1-2
- monitoring the process 1-12
- predetermined data diskette 1-2

initialization process, end of screen, illustrated 1-12

initialization tasks
- complete system configuration 1-13
- connect Ethernet cable or cables 1-8
- create configuration data diskette 1-4
- insert configuration data diskette 1-7
- monitor initialization process 1-11
- power up server 1-10
- preinitialization 1-2
- removing front bezel 1-6

Inspect Utility
- description C-11
- printing Inspect listing C-11
- running C-11
- starting remotely C-28

installing management software
- Compaq Insight Manager 5-15
- Compaq Insight Manager for HP OpenView (Windows 2000 operating system) 5-15
- Compaq Insight Manager for Tivoli NetView (AIX) 5-15

Integrated Management Log *See* IML

Integrated Remote Console, features C-26

integrated server management, features C-21

international regulations, compliance D-6

Internet Protocol (TCP/IP) Properties dialog box, illustrated 6-41

IP access C-28

IP/IPX, using network features C-24

J

Japanese Notice D-5

L

LAN (Local Area Network)
  access through NIC 5-4
laser
  device regulatory compliance notice D-6
  information D-7
  type D-7
laser device
  product label D-7
laser safety
  warning D-6
LED indicators
  hard drives 6-28
LEDs
  hard drive C-2
    activity 6-29, 6-30
    fault 6-29, 6-30
    online 6-29, 6-30
  power indicator 1-10
License Warning dialog box, illustrated 6-48
licensing 6-48
Lifeguard
  service 2-29
  using during restore, caution 2-29
Linux
  accessing other platforms 4-3
  Compaq Insight Manager for 5-14
  installing Insight Manager for Tivoli 5-15
  managing with 5-14
  Tivoli NetView 5-1
load balancing
  increasing 6-37
  teaming option
    adaptive load balancing 6-46
    with IP address 6-47
    with MAC address 6-47
Load Balancing Control teaming option, illustrated 6-46
Local Area Connection Internet Protocol Properties dialog box, illustrated 6-53
Local Area Connection Properties dialog box, illustrated 6-52, 6-54
local area network *See* LAN
logical drive
  caution 6-14, 6-22
logical drives
  caution 6-2
  deleting, caution 6-10
Logoff dialog box, illustrated 2-8
Low Voltage Differential *See* LVD
`ls -al` command, defined 4-11
LVD (Low Voltage Differential)
  defined A-4
LVM (Logical Volume Manager)
  caution 6-14
  described 6-14

M

management software, installing 5-15
management, using a Web browser 2-11
managing users and groups
  group names 3-54
  organization 3-2
  usernames 3-3
  using tags 3-54
map maintenance, illustrated 4-26
mapping
  changing primary 4-25
mapping server
  ls -al command example, illustrated 4-11
memory
  cache 6-6
  clearing NVRAM C-30
  ECC 6-6
  errors, recorded to log C-24

Microsoft Management Console *See* MMC. *See* MMC
Microsoft Windows file system security, website 3-55
MKS (Mortice Kern Systems) Toolkit
  defined 4-28
  SFU component 4-2
MMC (Microsoft Management Console)
  CIFS workgroup environment, managing users and groups 3-4
  CIFS, open file management 3-83
  Compaq Web Management 2-6
  Compaq Web Management components, listed 2-6
  console for file sharing administration 3-73
  core operating system 2-4
  defined C-37
  deleting shares 3-79
  described 2-3
  disk system 2-4
  disk system snap-ins, listed 2-4
  exporting snap-ins 2-5
  file exporting 2-5
  growing virtual disk 6-25
  hardware system snap-ins, listed 2-5
  managing CIFS sessions 3-82
  modifying shares 3-79
  NFS
    stopping and starting C-37
  Online Volume Growth Wizard, growing virtual disk 6-25
  snap-ins
    add/remove 3-16
    listed 2-4
  SWVR, growing virtual disk 6-24
  system 2-5
  user name mapping 4-10
MMC (Microsoft Management Console) screen, illustrated 2-3
Modify User Properties
  Account tab dialog box, illustrated 3-29
  General tab dialog box, illustrated 3-28
  Member Of tab dialog box, illustrated 3-33
  Profile tab dialog box, illustrated 3-32
  Sessions tab dialog box, illustrated 3-35
Modify User Properties, dialog, box, illustrated 3-8
Mortice Kern Systems Toolkit *See* MKS (Mortice Kern Systems) Toolkit
Mouse FCC compliance statement D-4
moving arrays
  array controller 6-34
  restrictions 6-34

N

NAS (network attached storage)
  backup solutions A-1
  capabilities A-1
NC3132 NIC LEDs
  troubleshooting with C-39
NC3134 NIC LEDs
  troubleshooting with C-39
NC6134 NIC LEDs
  troubleshooting with C-40
NET SHARE
  command, creating shares 3-70
  resources, listed 3-71
network access, configuring ASR-2 for C-28
Network and Dial-up Connections screen, illustrated 6-50
network attached storage *See* NAS
Network File System *See* NFS

Network Identification welcome dialog box, illustrated 3-42
Network Information Service *See* NIS
Network Node Manager *See* NNM
Network Properties dialog box, illustrated 6-51
New Global Group dialog box, illustrated 3-51
New Group, dialog box, illustrated 3-11
New Local Group dialog box, illustrated 3-52
New Object
  User dialog box, information summary, illustrated 3-25
  User dialog box, password information, illustrated 3-23
  User, user dialog box, user information, illustrated 3-22
New Object - Computer dialog box, illustrated 3-19
New Object - Group dialog box, illustrated 3-36
New Share dialog box, illustrated 3-85
New Snapshot Wizard screen, illustrated 2-18
New Technology File System *See* NTFS. *See* NTFS
New User dialog box
  User Manager for Domains menu, illustrated 3-44
New User dialog box
  account
    global 3-48
    local 3-48
    selecting 3-48
  Account button 3-48
  Dialin button 3-49
  groups 3-46
  Logon To button 3-48
  Profile button 3-47
New User, dialog box, illustrated 3-4
NFS
  stopping and starting
    from command line C-37
NFS (Network File System)
  auditing
    establish settings 4-32
    levels available 4-32
  authentication
    client level 4-5
    per-export basis 4-5
    squashing 4-5
  client groups 4-30
  compatibility with CIFS 3-88
  configurations 4-4
  defined 1-15, 4-3
  design goals 4-3
  double translation 4-11
  exporting procedures, using SFU 4-28
  fault tolerance 4-27
  file exporting, using SFU 4-28
  file locking
    advisory 4-31
    clearing locks 4-31
    user interface 4-31
  file service, stopping and starting C-37
  mapping server operation modes 4-10
  network protocols 4-4
  protocol combinations 4-4
  testing 4-29
  versions 4-4
NFS (Network File System) server
  component functionality 4-6
  former restrictions 4-6
  logging events 4-8
  SFU
    abilities 4-6
    integration 4-6
  user mapping 4-7
  Windows NT access 4-6
  Windows NT filesharing 4-6

NFS (Network File System) Server
  User Mapping, illustrated 4-7
NFS (Network File System) server, Logging pane, illustrated 4-8
NFS (Network Information Service)
  file locking, described 4-31
NIC (Network Interface Controller)
  troubleshooting C-38
NIC (Network Interface Controller) teaming
  troubleshooting 6-56
NIC Properties dialog box, illustrated 6-42
NIS (Network Information Service)
  configuration screen,
    illustrated 4-14
NIS (Network Information Service), defined 1-1
NIS (Network Information Service), multiple 4-26
NNM (Network Node Manager), defined 5-13
NTFS (New Technology File System) File Permission Entry, for file name screen, illustrated 3-56
NTFS (New Technology File System), security 3-55

O

OCU (Offline Configuration Utility), defined 5-6
Offline Configuration Utility *See* OCU
online volume growth
  adding storage to pools 6-22
  growing a virtual disk 6-24
  preparing disks 6-21
  preparing for 2-14
  SWVR feature,
    described 6-21
open file management
  closing
    a single open file 3-83
  closing all open files 3-83
  described 3-83
open files, disconnecting, caution 3-83
operating system, starting into C-29
ownership of files 3-68

P

parts
  handling E-1
  transporting E-1
password port configuration, synchronization 6-63
password synchronization
  advanced settings 6-61
  auditing 6-63
  default settings 6-63
  encryption key 6-63
  service
    auditing 6-63
    default settings 6-63
    encryption key 6-63
    port configuration 6-63
    sync retries 6-63
    UNIX to
      Windows NT/2000 6-63
  service port
    configuration 6-63
  sync retries 6-63
  UNIX to
    Windows NT/2000 6-63
password synchronization service
  described 6-62
  security 6-63

passwords
  Active Directory
    domain 3-23, 3-41
  changing at logon 3-5
  changing client 3-6
  configuring 3-5
  disabling C-30
  effects on configuration 6-59
  modifying 3-7
  new user, workgroup environment 3-5
  password synchronization service 6-62
  security 6-59
  setting, new user 3-4, 3-23
  synchronization 6-59, 6-62
    implementation 6-60
    requirements 6-60
    Windows Powered OS 6-59
  workgroup environment 3-5
passwords synchronization
  security 6-63
PC Network File System *See* PCNFS
PCNFS (PC Network File System)
  configuration screen, illustrated 4-15
PDC (Primary Domain Controller)
  defined 4-12
PDC (primary domain controllers)
  password
    synchronization 6-62
permissions
  administering 3-16
  NFS 4-28
  setting through Windows Explorer 3-85
  user level 4-9
  view from command line 4-33
personal injury
  warning C-2
personal injury, warning C-4
policies, managing user accounts 3-30
pools
  capacity expansion 6-35
  creating virtual disks 6-17
  creating with SWVR 6-14
  deleting 6-19
  large 6-35
  moving arrays 6-34
  New Pool Wizard 6-15
  online volume growth 6-21
  Snapshot Manager 6-14
  storage, described 6-2
port configuration, password synchronization 6-63
POST (Power-on Self-Test)
  messages
    drive positions changed 6-26
POST (Power-On Self-Test)
  messages
    array accelerator disabled 6-7
    re-enable logical drive 6-33
POST Power-On Self-Test)
  messages
    fault tolerance 6-33
power
  warning xi
power button, location 1-10
power outages 6-58, C-25. *See also* UPS
power source symbol xi
powering down the server 2-12
Power-On Self-Test (POST)
  messages
    drive failure 6-27
Power-On-Self-Test *See* POST
predictive failure alert
  defined C-6
  guidelines for drive
    replacement C-4, C-5, C-6, C-7
  how to implement C-6
primary domain controller *See* PDC. *See* PDC
Primary User Mapping applied, illustrated 4-25

properties
  guests 3-14
  modifying 3-28
    group 3-14
    user 3-8
  user, passwords 3-5

Q

QuickRestore
  configuring spares C-54
  description C-52
  full menu option C-53
    automatic C-53
    manual C-53
  Full Restore menu option C-55
  menu option C-54
  menu options, listing C-52
  post QuickRestore additional setup C-57
  post QuickRestore and automated setup C-56
  verification C-52
quotas
  auditing capabilities 2-32
  enabling
    drive quotas 2-32
    procedure 2-32
  managing space usage 2-32
  saving audits 2-32
  setting 2-32
  system administrator 2-32
  users 2-32

R

rack stability, warning xii
radiation
  warning D-6
RAID 0, fault tolerance B-3
RAID 1
  described B-3
  drive mirroring B-3
  drive mirroring, illustrated B-4
RAID 10
  fault tolerance B-3
  RAID 0+1+ B-3
RAID 4, described B-1
RAID 5
  compared to RAID 4 B-1
  described B-1
  distributed data guarding B-1
  distributed data guarding, illustrated B-2
  storage management 6-6
Rapid Recovery Engine, enabling C-21
Read permission level 3-76
Readme and Product Information, option 2-9
recovery
  attended C-23
  automatic C-22
  environmental C-22
  from software error C-22
  rapid error recovery services C-21
  unattended C-23
registering appliance, Active Directory domain 3-41
regulatory compliance, identification number D-1
remote administration
  Compaq Insight Manager
    Agent Web interface 5-11
    components 5-9
    console 5-10
    management agents 5-9
  enterprise management
    Compaq Insight Manager for HP OpenView 5-12
    Compaq Insight Manager for Tivoli NetView (AIX), Version 2 5-14
    HP OpenView 5-12

        installing software 5-15
        Tivoli NetView (Linux) 5-14
    management software
        Compaq Insight Manager for HP OpenView 5-15
    methods 5-1
    Remote Insight Lights-Out Edition board
        administration tasks 5-4
        capabilities 5-4
        configuration 5-6
        configuration changes 5-6
        default DNS name 5-6
        factory default settings 5-6
        features 5-4
        installation and users guide 5-4
        manage alerts feature 5-5
        manage users feature 5-5
        management functions 5-4
        OCU 5-6
        remote access 5-8
        Web interface 5-4
    Remote Shell Daemon 5-3
    Telnet Server
        auditing 5-2
        authentication 5-2
        sessions 5-3
        settings 5-3
Remote Insight Light-Out Edition board
    configuration 5-6
Remote Insight Lights-Out Edition board
    capabilities 5-4
    resetting C-46
    troubleshooting C-46
Remote Procedure Call *See* RPC
Remote Shell Daemon
    remote administration 5-3
resources
    Compaq Insight Manager C-6
    Compaq Management Agents for Servers C-6
    Compaq Management CD C-6
    predictive failure C-6
restart system, dialog box, illustrated 2-8
restarting the server 2-12
Restore From Snapshot Wizard
    Schedule Information dialog box, illustrated 2-25
    Snapshot Information dialog box, illustrated 2-22
    Task Information dialog box, illustrated 2-23
    User Identification for Scheduled Task dialog box, illustrated 2-24
RJ-45 receptacle symbol xi
ROM corrupted C-29
ROMPaq
    disaster recovery C-29
    error recovery options C-29
    Firmware Upgrade Utility
        accessing C-12
    Firmware Upgrade Utility, accessing C-12
    interruption C-29
RPC (Remote Procedure Call settings and statistics 4-33

S

safety information xi
SAN (storage area network)
    backup solutions A-2
    defined A-2
SANworks Virtual Replicator *See* SWVR
SCSI
    devices, troubleshooting C-8
    tape devices
        HVD A-4
        LVD A-4
        single-ended (SE) A-3
        types A-3
SCU (System Configuration Utility)
    accessing C-12
    defined C-12
    starting remotely C-28

SCU (System Configuraton Utility)
  selecting Diagnostics C-14
security
  CIFS and NTFS security integration 3-69
  integrating
    described 3-69
    local file system into Windows domain environments 3-69
  managing 3-60
  storing CIFS and NTFS file system permissions 3-69
  Windows file system 3-55
Security ID *See* SID
security levels
  Caution C-19
  Critical C-19
  Repaired C-19
  Status C-19
Security Properties dialog box
  options 3-60
Security Properties dialog box, for folder name NTSF Test, illustrated 3-60
Select Domain dialog box, Administering Users and Groups, illustrated 3-43
Select Domain dialog box,Server Manager, illustrated 3-38
Select Groups, dialog box, illustrated 3-10
Select User, Computer, or Group dialog box, illustrated 3-66
Select Users or Groups, dialog box, illustrated 3-12
Selected Logical Drives dialog box, illustrated 6-16
series number, regulatory compliance D-1
server
  powering up, illustrated 1-10
Server for NFS
  installation on a domain controller 4-13
Server Message Blocks *See* SMB
server response, troubleshooting slow C-3
Services for UNIX *See* SFU. *See* SFU
Set Password, dialog box, illustrated 3-7
set primary user mapping, illustrated 4-24
SFU (Services for UNIX)
  described 4-1
  mapping users 1-14
  server for NFS 4-6
  troubleshooting C-31
  user name mapping 4-9
SFU (Services for Unix) for NFS file locking, illustrated 4-31
SFU (Services for Unix) Password Synchronization dialog box, illustrated 6-59
SFU (Settings for Unix) Password Synchronization dialog box, advanced settings, illustrated 6-61
SFU screen user interface, illustrated 4-1
Share Properties dialog box, General tab, illustrated 3-79
shares
  accessing 3-1
  administering through Windows Explorer 3-84
  administrative 3-88
  creating
    command line 3-70
    methods 3-70
    NET SHARE command 3-70
    with MMC 3-72
  cross-platform management 3-88
  deleting
    with MMC 3-79
  deleting with Windows Explorer 3-86

- modifying
  - with MMC 3-79
- modifying with Windows Explorer 3-87
- permission levels
  - listed 3-76
- setting up through Windows Explorer 3-84
- standard 3-88

Shutdown system, option 2-9
Shutdown, dialog box, illustrated 2-9
SID (Security ID), defined 4-9
simple maps for NIS
- Show User Maps dialog box, illustrated 4-18

simple maps for PCNF
- Show User Maps dialog box, illustrated 4-16, 4-17

simple maps in mapped users list for NIS dialog box, illustrated 4-19
sizing tools, backup
- described A-2
- direct connection A-2
- enterprise solutions white paper A-2
- fibre connection A-2

Smart Array Controller
- benefits 6-6
- features 6-6
- four-port 6-6
- hot-plug guidelines C-5, C-6, C-7
- integrated 6-6

Smart Array Controller Configuration Utility, preview dialog box, illustrated 6-10
SmartStart
- Support Software CD
  - contents C-12
  - running utilities C-12, C-13

SMB (Server Message Blocks), described 3-1
snap-ins
- adding and removing 3-16
- connecting to domain 3-18
- disk system 2-4
- MMC 3-16

Snapshot Manager interface, illustrated 6-17
Snapshot Manager screen
- deleting a virtual disk, illustrated 6-20
- deleting snapshots, illustrated 6-19
- scheduling snapshots, illustrated 2-27

Snapshot Manager screen, illustrated 6-15
Snapshot Managerscreen
- creating snapshots, illustrated 2-17

snapshot recovery
- caution 2-20

snapshots
- access 2-19
- backup 2-19
- benefits 2-15
- caution 2-29
- creating 2-16
- creating, managing, and scheduling 2-15
- drive defragmentation 2-26
- effects on virtual disk 2-15
- facts, listed 2-16
- initially implementing 2-25
- pool sizing 2-25
- read performance 2-15
- recurring 2-28
- restoring a virtual disk 2-20
- restoring files and directories 2-20
- running backups 2-28
- scheduling 2-27
- Snapshot Planner utility 2-25
- snapshots of 2-19
- virtual disks 2-26

- Windows 2000
    - defragmenter 2-26
  - write locality 2-15
  - write performance 2-15
- software error
  - recovery C-22, C-25
  - recovery start option C-25
  - recovery timeout C-25
- software vendors, backup solutions A-5
- space management process, illustrated 6-3
- standby recovery
  - server option C-25
  - server port C-25
  - time out C-25
- storage area network *See* SAN
- storage enclosure
  - power down precaution 6-27
- storage management
  - ACU 6-4
  - default settings 1-15
  - features 6-2
  - RAID 5 6-6
  - Smart Array Controller
    - described 6-4
    - features 6-6
- storage units
  - adding to array 6-22
  - adding to pool 6-23
- Survey Utility, viewing C-20
- SWVR (SANworks Virtual Replicator)
  - creating pools 6-14
  - defined 6-14
  - described 2-12
  - growing virtual disk 6-24
  - Lifeguard service 2-29
  - modify reserved pool space 2-30
  - online volume growth 6-24
    - adding storage to pools 6-22
    - described 6-21
    - preparing disks 6-21
  - storage tools
    - listed 2-12
    - online volume growth 2-14
    - snapshots 2-13
    - storage pooling 2-13
    - virtual disks 2-13
- symbols
  - in text x
  - on equipment x
- synchronization *See* password synchronization
- synchronization, password 6-59
- System Configuration Utility *See* SCU
- System Tools menu, selection screen, illustrated 6-9

T

- tables
  - Access Level Description 3-58
  - Access Level Permissions 3-57
  - Active Directory User Account Characteristics 3-24
  - ASR-2 Features C-25
  - Caching Settings 3-81
  - Command Line Interface Command Prompts 4-33
  - Configuration Switches C-30
  - Data Drive Groups 6-5, C-53
  - Ethernet Network Connectors 1-9
  - Group Name Examples 3-54
  - Hard Drive LED Combinations 6-29
  - Hard Drive Problems C-3
  - Managing User Account Properties 3-30
  - MMC Subfolders 3-72
  - NC 6132 NIC LEDs C-40
  - NC3132 and NC3134 NIC LEDs C-39
  - NET SHARE Resources 3-71

- New User Check Boxes 3-5
- NIC Teaming
  - Troubleshooting 6-56
- Primary Processor Test Error Codes C-16
- Storage Enclosure Drive Bay Configuration for Replacing Failed Hard Drives 6-31
- TaskSmart N2400 Server
  - Troubleshooting C-8
- Windows NT Server 4.0 User Account Characteristics 3-45

Taiwanese Notice D-5

tape backup connection methods
- described A-3
- Fibre Channel A-4
- SCSI, direct A-3
- SCSI, implementing A-3

tape devices, backup solutions A-2

TaskSmart N2400 console
- administrative management 2-2
- overview 2-2
- tasks
  - command prompt 2-7
  - halt system 2-9
  - Help 2-10
  - listed 2-2
  - logoff 2-8
  - restart system 2-8

TaskSmart N2400 Console, illustrated 2-2

TaskSmart NAS Management dialog box
- CIFS Session manager using MMC, illustrated 3-82

TaskSmart NAS Management dialog box
- Open Files manager using MMC, illustrated 3-83

TaskSmart NAS Management MMC consol for file sharing administration, illustrated 3-73

TCP (Transport Control Protocol), with NFS 4-4

Teaming Controls dialog box, Fault Tolerant option, illustrated 6-44

technical support
- Compaq phone number xii
- obtaining xii
- website xii

telephone symbol xi

Telnet Server
- defined 5-2
- interface screen, illustrated 5-2
- remote administration
  - auditing 5-2
  - authentication 5-2
  - sessions 5-3
  - settings 5-3

text conventions, described ix

thermal shutdown C-25

Tivoli NetView (AIX), remote administration 5-14

Tivoli NetView, remote administration 5-9. *See also* third-party software

Transport Control Protocol *See* TCP

troubleshooting *See also* QuickRestore
- cannot export C-31
- checklist C-2
- hard drives C-2, C-5, C-6
- Hewlett Packard (HP) OpenView C-52
- incorrect event log entries C-51
- keyboard and mouse C-51
- LED error codes C-51
- logon issues C-47
- methods C-48
- miscellaneous
  - incorrect ROM C-58
- NIC C-38, C-40, C-42

- NIC (network interface controller) C-38
- NIC (network interface controller) LEDs C-39, C-40
- NIC teaming 6-56
- NICs C-40, C-41, C-43, C-44
- overview C-1
- QuickRestore C-52
- Remote Insight Lights-Out Edition board C-46
- Remote Insight Lights-Out Edition board, network interface C-49
- SCSI devices C-8
- server
  - cannot be pinged C-8
  - not working C-8
  - will not start C-8
- SFU
  - folder names with spaces and underscores C-33
  - mapping changes not reflected C-36
  - mapping multiple users C-34
  - mounted logged out client C-34
  - mounting UNIX clients C-35
  - permission denied error C-33
  - root permissions C-32
  - RPC, showmount, or other commands C-32
  - shared folder problems C-33
  - shared out error messages C-34
  - user identification problems C-31, C-32
- slow server response C-3
- SNMP trap parameters C-50
- Web browser, software C-49

troubleshooting, 30% pool space for snapshots C-58
troubleshooting, Compaq Insight Manager C-59
troubleshooting, external storage system C-58
troubleshooting, hard drive, memory, or processor failure C-59
troubleshooting, power supply failure C-58
troubleshooting, system event log C-58
Tru64 UNIX, accessing from Linux 4-3

U

UDP (User Datagram Protocol), with NFS 4-4
UID (user ID)
- authentication 4-5
- defined 4-9

uninterruptible power supply *See* UPS
UNIX identification mechanism 4-9
UPS (uninterruptable power source)
- power outages C-25
- shutdown C-25
- shutdown threshold C-25

UPS (uninterrupted power source)
- automatic power-down 6-58
- battery power supply 6-58
- defined 6-58
- options 6-58
- power outages 6-58
- protection 6-58
- required 6-58
- serial line connection 6-58
- using 6-58

User Datagram Protocol *See* UDP
User Environment Profile dialog box, illustrated 3-47

user guides
  Fast Ethernet and Gigabit NIC 2-10
  Remote Insight Lights-Out Edition board 2-10
  Server Online Reference 2-10
  Smart Array 5300 2-10
  SWVR 2-10
user ID *See* UID
user ID (UID), defined 4-9
User Manager for Domains 3-43
user name mapping
  advanced mode 4-11
  automatic 4-14
  backup and restoration 4-26
  creating primary 4-24
  explicit 4-19
  from different deployment of services 4-27
  guidelines
    advanced 4-14, 4-19
    simple 4-14, 4-15, 4-17, 4-20
  implementation 4-10
  implicit 4-14, 4-15, 4-17, 4-20
  limitation 4-12
  manual 4-19
  mapping procedures 4-12
  matching spellings 4-14
  NIS 4-17
  PCNFS 4-15, 4-20
  requirement 4-12
  security rights 4-9
  SFU 4-9
  simple mode 4-10
  simulate redundant mapping servers 4-27
  source of mapping
    CIFS 4-12
    UNIX 4-12
  user access 4-9
  user level permissions 4-9
User Name Mapping user interface, illustrated 4-10
User or Group Permission Entry dialog box, for folder name NTSF Test, illustrated 3-63
user properties
  changing 3-8
  dial-in 3-9
  disabling account 3-8
  locking account 3-8
  member of 3-9
  modifying 3-8
  profile 3-9
User Properties dialog box, Member Of tab, illustrated 3-9
UserData Properties dialog box, Sharing tab, illustrated 3-84, 3-87
usernames, managing users and groups 3-3
utilities
  accessing C-12
  ACU
    accessing C-12
  ACU, accessing C-12
  ADU, accessing C-12
  ASR-2 C-28
  backup solutions
    archiving A-6
    developing A-2
    disaster recovery A-9
    Fibre Channel A-4
    media rotation A-8
    multiple backup devices A-8
    offsite storage A-1, A-8
    readiness testing A-8
    regular backups A-6
    schedules A-7
    SCSI, direct-connect A-3
    SCSI, implementing A-3
    software vendors A-5
    tape devices A-2
    tape devices, connection methods A-3
    through SAN A-2

backup tools
  considerations A-2
  direct connection A-2
  fibre connection A-2
  sizing, enterprise solutions white paper A-2
  website resources A-2
command line 2-7
Compaq
  running on IPX network C-24
  running remotely C-24
Compaq Survey C-20
CPQTEAM 6-37
creating diskette versions C-13
Diagnostics
  accessing C-12
  Compaq system partition C-12
  menu choices C-14
  SCU C-14
firmware upgrade, accessing C-12
Health Driver C-26
IML Management Utility, described C-20
Inspect
  description C-11
  printing Inspect listing C-11
  running C-11
ROMPaq C-12
running from SmartStart and Support Software CD C-13
Survey, described C-20
System Configuration, accessing C-12

V

virtual disk
  growing
    from SWVR 6-24
virtual disks
  creating from pools 6-17
  defragmenting 2-26
  deleting 6-19
  growing
    MMC 6-25
  growing from Online Volume Growth Wizard 6-25
  snapshots 6-17
volume growth
  virtual disk 6-24
volume growth, SWVR feature 6-21
volume growth, virtual disk 6-25

W

warnings
  batteries D-8
  defined x
  electric shock x, xi
  hazardous radiation D-6
  hot surface xi
  laser safety D-6
  multiple power sources xi
  personal injury C-2, C-4
  rack stability xii
  weight xi
Web browser, management 2-11
Web Enabled interface, illustrated 5-13
Web user interface, remote administration 5-8
websites
  ActiveAnswers 3-15, 3-21, 3-36
  backup tools A-2
  Compaq xii, xiii
  Windows file system security 3-55

weight
  symbol xi
  warning xi
Windows Explorer
  administering CIFS shares 3-84
  deleting a CIFS share 3-86
  modifying a CIFS share 3-87
  setting caching 3-85
  setting permissions 3-85
  setting up shares 3-84
Windows file system security
  described 3-55
  website 3-55
Windows NT Server 4.0
  account properties 3-48
  adding a user 3-44
  administering users and groups 3-43
  creating an account 3-39
  creating new global group 3-51
  deleting a user 3-49
  domain, described 3-37
  Global Groups 3-49
  launching Server Manager 3-37
  Local Groups 3-49
  logon access 3-48
  modifying a user profile 3-47
  modifying a username 3-49
  modifying group 3-51
  modifying user properties 3-49
  Server Manager 3-37
  user manager 3-49
Windows Powered OS
  password
    synchronization 6-59
Windows user and UNIX user
  to map and add for PCNFS dialog box, illustrated 4-21
Windows users and UNIX users
  to map and add for NIS dialog box, illustrated 4-23
wizards, ACU 6-4
  bypassing 6-36
workgroup environment
  compared to domain 3-2
  group administration
    adding a group 3-11
    adding users or groups 3-12
    deleting a group 3-13
    guest properties 3-14
    modifying a group 3-13
  new user
    password 3-5
    setting password 3-4
  user administration
    adding a user 3-4
    changing a client password 3-6
    deleting a user 3-6
    modifying a password 3-7
    modifying a user 3-6
    modifying properties 3-1, 3-8
wrist strap, using E-2